IMPERIAL MUNICIPAL PARTNERS
154 East Main St, (Rte. 16), Milford, Mass. • 508-422-1000

October 29, 2013

Lieutenant Thomas Fitzgerald
Massachusetts State Police
Commercial Motor Vehicle Enforcement Unit
906 Elm Street
Concord, MA 01742

REF: PROPOSAL - Mobile ALPR Unit

Thank you for the opportunity to provide you with a quote on the 3M formerly PIPS Mobile ALPR system. This proposal includes pricing for a three camera ALPR mobile system permanently installed on a Ford Expedition slick top. It is understood that the existing BOSS server software plus Bing Maps utility presently in operation at EOPS/Chelsea will be used to support this proposed system. The mobile ALPR units will have access to PRISM, NCIC and Registry Motor Vehicle ALPR hotfiles.

Key points about PIPS (3M) in the ALPR market:

- For more than 20 years 3M formerly PIPS' focus has been specializing in Automatic License Plate Recognition technologies and is considered by many as the industry pioneer in this market.
- As an Original Equipment Manufacturer, 3M, manufactures, and develops it's own hardware and software – and control the quality and support of their products from start to finish.
- 3M offers an ALPR "back-end" analysis software package (BOSS) that provides data-mining of "historic" license plate information obtained and stored from all deployed mobile (and fixed) systems within your department.

PROPOSAL

Item	Qty.	Description	List Unit Cost
1	[redacted]	SLATE-750-LE-G: Three Camera Mobile Law Enforcement Package including 750nm illumination, SupeRex processor, camera cable/connector(s), GPS module,PAGIS software, PIPS ALPR/OCR Engine, Client/Server architecture, camera bracket mount assemblies, three year warranty	[redacted] TOTAL $468,125
2		Two Concurrent User License	
3		PIPS-SW-BOSS Back Office System Software & Mapping utilizing Microsoft SQL Express Server Software for system administration, data analysis and data storage,	$N/A Assumed existing BOSS Software

		data mining, reporting, mapping via the Bing Maps Utility, remote alerting, and networking in support of inter-agency data sharing.	located at Chelsea will be used
4	G.L. c. 4.sec. 7.cl.26 (f) [redacted]	**INSTALLATION**; Installation, Training, Optimization, IT configuration	G.L. c. 4.sec. 7.cl.26 (n)(sec [redacted] TOTAL $40,000
		TOTAL	**$508,125**

Scope of Work:

Our quote ***includes*** mobile installation on a Ford Expedition, and software implementation and training into the existing BOSS software at Chelsea-EOPS. BOSS for your agency can be utilized for all future PIPS mobile or fixed installations within your organization.

NOTE 1: If you are running NetMotion for your MDC, you will need version 10.0 or higher with the Policy Manager License (extra add-on license above and beyond the standard NetMotion server license offered by NetMotion). Refer to NetMotion Tech Note # 2200.

NOTE 2: MDT Minimum Requirements:

These are minimum specifications provided by the manufacturer. Experience with those agencies that have MDT's with minimum specifications may experience operating issues such as slow response in processing speeds, and periodic freezing of the operating system.

- 1.8 GHz AMD or Intel Processor with 2GB of Memory with 128MB available for PAGIS.
- Windows XP Pro with Service Pack2 or later.
- Available 10/100 Ethernet Port and USB Port (1.1 or higher - 2.0 preferred).
- 15 GB available space on the hard drive.
- XVGA screen with minimum of 800x600 screen resolution. Touch screen preferred.
- Wireless connectivity

NOTE 3: All PIPS equipment hardware and software is covered by a one-year parts and labor warranty. Extended warranty agreements are available for the system after the original one-year warranty expires. These agreements supply the end user with upgrades and improvements to our OCR engine for enhanced plate detection capabilities and PAGIS and BOSS software upgrades.

-

Mobile / Unit Extended Maintenance & Support Per System – Hardware / Software / OCR (Year 1 included in purchase)	Unit Cost
Each Additional Year – Annual Mobile System Maintenance Renewal	$1325

Please let me know if you have any questions or require any additional information.

Thank you in advance,

Clay Chase
President

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).

2017 National Fusion Center Association Annual Training Event Alexandria Hilton—Mark Center

November 7–9, 2017

Roadmap to Our Sponsors

Greetings, **2017 National Fusion Center Association (NFCA) Training Event** Attendees!

We look forward to welcoming you to our annual NFCA training and networking opportunity in just a few days—**November 7–9**—at the **Hilton Alexandria Mark Center hotel**.

Thank you for your collaborative commitment to the National Network of Fusion Centers and to safeguarding our neighborhoods and securing our Nation through your dedication:

- As critical members in the fusion center, intelligence, and analyst communities.
- As force-multiplying partners and stakeholders.
- As private sector innovators.

To gear up for productive and enjoyable engagements, we are pleased to provide this ***"Roadmap to Our Sponsors,"*** highlighting products and services from our premier industry supporters. Please take a few minutes to preview the impressive range of offerings, and plan to tour the Sponsorship Showcase lobby area for further exploration and face-to-face conversations. **The Sponsorship Showcase floorplan is included as the last pages of this resource.**

We can't wait to see you there!

NFCA Training Event Planning Team
Donna Jean Lindquist
Communications
E-mail: dlindquist@iir.com
Learn how the National Fusion Center Association is helping protect America at https://nfcausa.org/.

THE SCIENCE OF WHERE™

Platinum Sponsor

Booth: **100**

Overview: **ONE PLATFORM, MANY MISSIONS**

Esri® ArcGIS® software provides a framework to integrate all types of data, sensors, and activities in real time to understand and share actionable intelligence to make your community safe.

Learn more at: **go.esri.com/NFCA2017**

Awards Sponsor

Booth: **121**



CARFAX®
CARFAXFORPOLICE.COM

Gold Sponsor

Booth: **103**

Overview: CARFAX has partnered with thousands of law enforcement agencies for more than 30 years to help solve crimes and keep communities safer. Get access to CARFAX's unique, proprietary database of more than 18 billion vehicle history records from more than 100,000 sources. Each day, 5 million records are added to the CARFAX database. Your agency's investigators/analysts can access this information at **no cost** to assist in their investigations and research.
Only CARFAX can provide you with the most comprehensive vehicle history data available in North America.

Stop by! Learn how over 48 Fusion Centers partnered with CARFAX are solving crimes faster . . .

- Conduct a Nationwide ***Partial License Plate Search*** within seconds
- Get 24/7 Surveillance of ***Vehicles of Interest***, Only from CARFAX ***(VIN Alert)***
- Mission Critical Information, Anywhere Detectives/Analysts Need it ***(Mobile App)***
- Access Nationwide Millions of ***Crash Reports***
- Receive Monthly ***High Mileage Reports*** on Suspected Stolen Vehicles

Ask for: **Mikeal Johnston: (571) 458-6419**; **mikealjohnston@carfax.com**

Preview at: **https://carfaxforpolice.com**

MSAB
When you want to stay ahead

Gold Sponsor

Booth: **123**



FirstNet™

Gold Sponsor

Booth: 120



VERITONE government

Gold Sponsor

Booth: 115

Overview: **Accelerate Investigations, Solve Cases Faster**

Effectively analyze and exponentially leverage more of your audio and video assets to speed investigations. Veritone helps you fulfill your mission by harnessing the cumulative powers of AI cognitive engines such as face recognition, object recognition, optical character recognition, transcription, translation, and more.

With Veritone, you can:

- Search content by faces, objects, spoken words, logos, and more
- Rapidly identify known offenders from video recordings and arrest photos
- Centralize data access to eliminate silos

Stop By! Visit **Veritone** at **Booth 115** to see the platform in action.

Preview at: **https://www.veritone.com/solutions/government/**

Thomson Reuters CLEAR

Silver Sponsor

Booth: **102**

Overview: Thomson Reuters CLEAR® is designed to meet the unique needs of your investigations by bringing relevant content into a single interface, allowing you to search data and view results in a way that matches how you work. Trusted by agencies nationwide for their most critical investigations, CLEAR gives investigators needed access to the most up-to-date public records data. With unique features specifically designed for investigators, like real-time incarceration and arrest gateway and license plate recognition data, you can stay one step ahead of criminals.

Stop By! **View an on-site demo** to see the latest in data and analytics.

Learn more at: **legalsolutions.com/CLEAR/Law-Enforcement**

Silver Sponsor

Booth: **116**

Overview: Following on from its acquisition of security Command & Control software manufacturer icomply Ltd, Veracity has been demonstrating VIEWSCAPE Pro™, an integrated security management platform which provides a unified and coherent system for management and control of single or multiple sites, allowing system operators to be far more efficient in responding to incidents. VIEWSCAPE Pro is fully integrated with Veracity's TRINITY™ direct-to-storage system and, fundamental to that, the award-winning, advanced COLDSTORE™ surveillance storage system. It also features a full video and media wall display option which can be reconfigured on-the-fly and in response to specific incidents or emergency situations. Live views may be mixed with playback and media streams such as broadcast news, online data streams, maps, or other graphical displays.

"Our end-to-end solution brings a new level of cost-effectiveness to the integrated Command Control system market" says Scott Sereboff of Veracity USA. "COLDSTORE has already established itself as the most reliable and cost-effective long-term storage solution available, and the addition of VIEWSCAPE Pro to our portfolio brings significant added-value for any project. The system can provide integration with access control, building management, intruder detection, VOIP intercom systems, and video analytics including LPR and facial recognition" added Sereboff. "A number of native security functions can be added to the system in a modular, customizable way, such as guard tour, lone worker monitoring, dispatch, alarm monitoring, and key management."

Stop By! **Check out our VIEWSCAPE Pro demo at Booth 116** and be entered to win Amazon Alexa and Echo Dot package!

Ask For: **Rony Batagower or Brett Miller**

Preview at: **http://www.veracityglobal.com/**

Silver Sponsor

Booth: **105**

Overview: **Get the right message, to the right person, at the right time**

Are you looking for next generation digital solutions for mission critical communications? From real-time situational reports to social media photos and videos, law enforcement has never had to deal with so much information, from so many places, at the same time. How do you cut through the noise to ensure that critical information is captured? How do you manage the data to reveal insights and share them with the right person, at the right time?

Adobe's digital solutions can help fusion centers securely and efficiently share crucial information, while allowing you to focus on the important matters—protecting people and our communities.

Learn how Adobe is helping Law Enforcement Agencies:

- Enable cross agency secure collaboration and communication
- Manage video with tagging solutions and redactions
- Secure content and improve information sharing
- Expand the HSIN platform to easily create, deploy, and track virtual training

Learn more: If you are attending the National Fusion Center Association Annual Training Event in Alexandria, Virginia, stop by our Booth #105 or visit **adobe.com/government**

Silver Sponsor

Booth: **107**

Overview: **Information Management Solutions for Law Enforcement**

ACISS provides a complete investigative solution to automate the information flow from the initial Tip through the Investigative Case & Reports, Telephone Analysis, and Arrest.

ACISS Fusion is our information sharing framework which includes SAR integration with the Nationwide Suspicious Activity Reporting Initiative and the FBI eGuardian system. Approved SARs can be automatically exported in a LEXSPD-compliant XML format for transmission directly to the eGuardian web service.

The ACISS Command Module can automate the information flow in a Command Center for High Profile Criminal Incidents such as Bombings, Child Kidnappings, Homicides, etc. With the Mobile Field Interview Report (FIR), Tablets and Smartphones allow the investigator in the field to collect information and submit it directly to the Command Center.

Learn more at: **https://aciss.com/**

Vision Logic
Vigilance for the 21st Century

Silver Sponsor

Booth: **108**

Overview: Co-founded by "America's Crime Fighter," John Walsh, Vision Logic delivers the most comprehensive suite of analytics available today. From traditional video analytics to the latest capabilities in omni-directional audio analytics, Vision Logic is leading the way for the next generation of automated, real-time event detection and threat reduction solutions. Our solutions are deployed globally in over 120 different locations in 45 countries and include:

- Facial Recognition on Body Cams
- Automated Video Enhancement
- ALPR on Drones
- Multi-Factor Detection/Notification
- Omni-Directional Audio Analytics
- Air Quality Analytics
- Advanced Abandoned Object
- Remote/Mobile Surveillance



A Portion of all Revenue Goes Directly to the National Center for Missing & Exploited Children

Check Us Out: Swing by to see a live demonstration of the world's most robust Facial Recognition software…designed from the ground up to detect non-cooperative subjects in uncontrolled environments.

Look For: **Lou, Graham, or Rick**

Get the Latest: **www.vision-logic.com**

VIGILANT SOLUTIONS

Silver Sponsor

Booth: **122**

Overview: Vigilant Solutions investigative platform helps law enforcement solve crimes faster. Our easy-to-use interface was designed by former detectives combining analytics with license plate recognition (LPR) and facial recognition to generate more leads for investigating Part I and Part II crimes, as well as crime and intelligence analysis. Securely share real-time data nationwide among over 1,000 agencies, and tap into our exclusive commercial LPR database of more than 6+ billion vehicle detections. Combine your mugshots with our hosted facial recognition gallery and image editing tools to boost potential match searches. Bring criminals to justice with Vigilant Solutions.

Ask for: **Mark Rivera**, Customer Retention Manager
Bill Geraghty, Regional Sales Manager

Learn more at: **www.vigilantsolutions.com**

YOUR PARTNER FOR INVESTIGATIVE DATA

Silver Sponsor

Booth: **111**

Overview: Whooster delivers investigative data solution tools to law enforcement and government agencies alike who require real-time delivery of accurate data. Through SMS/Text Messaging, Web Based, Batching, Direct Connect and Integrated SaaS Solutions**—our** Whooster Data Fusion technology delivers the freshest, most reliable data needed for enforcement and regulatory concerns. Law enforcement investigations require the ability to identify and locate persons, detect patterns, and create comprehensive, actionable intelligence. Whooster LE data products deliver the information you need by filtering through billions of records to obtain the most up to date information in the market. Currently partnering with more than 900 law enforcement divisions, our proprietary technology is unique within the industry—allowing you to acquire actionable intelligence within seconds.

Close Cases Faster

Stop by to learn about the newest additions to our product offering of **social media, online ads and international capabilities including Mexican data**. The combination of these products are packing a powerful one two punch for our agency clients. Join the Whooster family of agencies successfully closing cases faster.

Federal and DOD Agencies—Now available for procurement through GSA!

Before you arrive: Try us out before you get to the event. **Get your free trial of Whooster at www.whooster.com.**

Stop by and see us! See Whooster in ACTION and why it is different. Register for our raffle for a $100 Amazon gift card.

ANOMALI®

Silver Sponsor

Booth: **119**

Overview: **Cyber No-Fly List**

The Anomali suite of threat intelligence solutions empowers organizations to detect, investigate, and respond to active cybersecurity threats. The award-winning ThreatStream threat intelligence platform aggregates and optimizes millions of threat indicators, creating a "cyber no-fly list." Anomali integrates with internal infrastructure to identify new attacks, or search forensically over the past year to discover existing breaches, and enables security teams to quickly understand and contain threats. Anomali also offers STAXX, a free tool to collect and share threat intelligence, and provides a free, out of the box intelligence feed, Anomali Limo. To learn more, **visit www.anomali.com** and **follow us on Twitter: @anomali.**

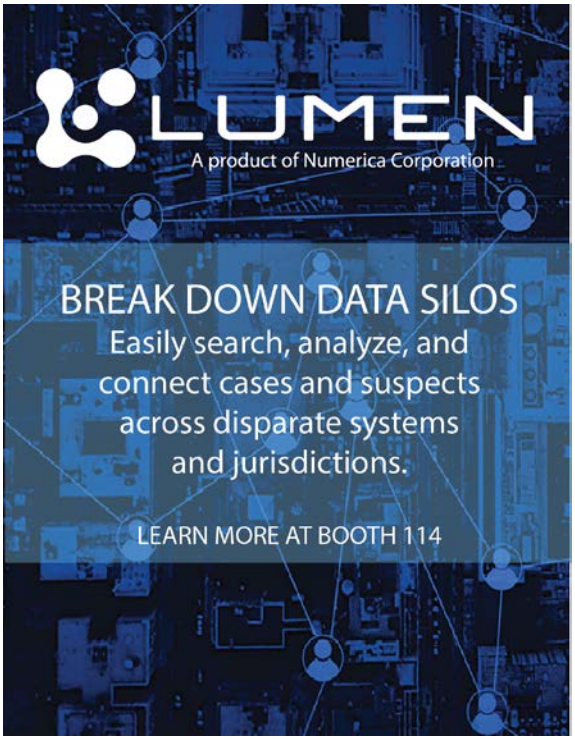
Learn more at: **www.anomali.com**

LUMEN
A product of Numerica Corporation

Silver Sponsor

Booth: **114**

Overview:



Haystax TECHNOLOGY

Silver Sponsor

Booth: **104**

Overview: **Come visit us at Booth 104**

For more than 18 years, Haystax Technology (formerly Digital Sandbox) has been helping federal, state, and local agencies share threat intelligence, maintain public safety, protect critical assets, and respond to natural disasters.



Stop By! For a **personal demonstration** of our cloud-based suite of **integrated applications for domain threat awareness and intelligence sharing.**

Ask for:
Jason Carroll, Doug Pasley, Melissa Follstad, Joe Lutz, or Brett Kozisek

You can also get **a preview** of our full suite of apps at **haystax.com**.

Silver Sponsor

Booth: **124**

Overview: **See the Big Picture**

Visit us in booth 124 to learn how you can display multiple sources of visual intelligence in one big picture view.

- Our software powers next-generation video wall and distributed visualization systems that are used to enhance situational awareness, establish a common operational picture, and improve collaboration.
- Hiperwall is a software-based and hardware-agnostic solution, resulting in lower cost, greater flexibility, a faster install and built-in ease of use. It enables you to:
  - Change views of visual intelligence of your choice, such as live video feeds, real time data, maps and custom applications for fusion centers, quickly, easily, and as often as you prefer;
  - Easily set up pre-set environments to display with a click of a button when local, regional, or national events occur;
  - Distribute content on multiple video walls and satellite displays located within a room or throughout a building; and
  - Send visual intelligence between Hiperwall systems located remotely, such as in outside agencies or other fusion centers.

Case studies: Learn how fusion centers have benefitted from Hiperwall! **Read KCTEW and WSIN**.

Schedule a demo at the Event: Contact **Richard Matthews at (949) 335-7420, x856 or rmatthews@hiperwall.com.**

Learn more at: **www.hiperwall.com**

Silver Sponsor

Booth: **118**

Overview: **TrapWire Fusion Center Intelligence Platform**

The TrapWire Threat Detection and Analysis Platform currently serves more than 2,000 public, private, military and Fusion Center sites across the U.S. The TrapWire system enables law enforcement officers and analysts to collect and analyze large volumes of incident and suspicious activity reports to detect indicators of planned terrorist or criminal activity. Our National Network links jurisdictions, organizations, and private-public partnerships into a common operating environment for the collection, analysis, and sharing of threat intelligence for law enforcement and critical infrastructure.

TrapWire utilizes report matching algorithms, artificial intelligence, and SME-designed analytical tools to detect threats in the planning stages.

Stop by! **Booth 118 for a demo and discussion with one of our threat experts**.

Ask For: **Dan Botsch**, President, or **Paul Chadha**, Director of Products and Technology

Learn more at: **http://www.trapwire.com**

neustar

Silver Sponsor

Booth: **117**

Overview: **Neustar's iTACT and IP Intelligence: THE Sources of Crucial Information for Law Enforcement Intelligence**

Does your team waste critical time chasing inaccurate location and contact information? Speed up your investigative process with data you can't find elsewhere—inclusive of household and business contact information across the U.S. and Canada.

iTACT—Neustar's Web-based intelligence portal—provides quick search for investigating phone numbers and finding additional phone numbers associated with an address. At the most critical moment, you can identify and verify names, addresses, and phone numbers, preventing inaccuracies and costly delays. iTACT also provides information on Vehicle Identification Numbers (VIN)—make, model, year, owner/owner addresses if needed.

Neustar's IP Intelligence is the authoritative source of IP data on 99.99% of routable IP addresses worldwide. IP Intelligence provides geographical, network, and proxy data that can further be used to support Law Enforcement with cybercrime investigations. With IP Intelligence, you can be confident that you are using the highest quality IP data available.

Stop By! **Come to booth 117 to understand how Neustar can help you accelerate your investigations.** Whether you need real-time or on-site access, Neustar's iTACT and IP Intelligence arms you with the information necessary to make the right decision at the right time. Our unique sources and hard-to-find data guarantee that there is no better source for your mission-critical intelligence. With unmatched speed and accuracy, you will accelerate investigations with precision.

Ask For: **Andrew DeBoissiere**, Senior Account Executive
(202) 236-9835 ♦ Andrew.DeBoissiere@team.neustar

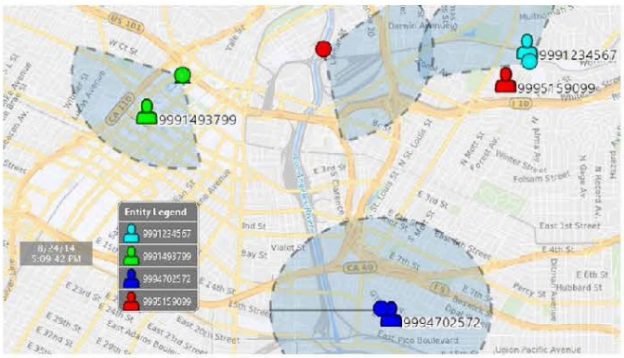
Learn More: **www.ipi.neustar**

Kind words from Mike Sena, NFCA President

"GeoTime has helped improve our analysts' ability to tell the story of criminals and the cellular devices they use. Before we had GeoTime, it would take days to develop the visual presentations that law enforcement, juries and the courts could understand. GeoTime has made us more efficient and effective."

Silver Sponsor
GeoTime® by Uncharted®
Booth: 110
Overview: GeoTime for law enforcement - Award-winning tool for formatting, analysis, mapping, and presentation of call records and mobile forensics data. Currently used by HIDTAs, fusion centers, national defense, and law enforcement agencies worldwide for criminal investigations, intel analysis, surveillance operations, and courtroom presentation.

See how easy it is to format, analyze, map, and create a courtroom presentation. Discover for yourself why your peers use GeoTime. Learn how GeoTime is used for investigations – homicide, burglary rings, missing persons, drug trafficking, and more.

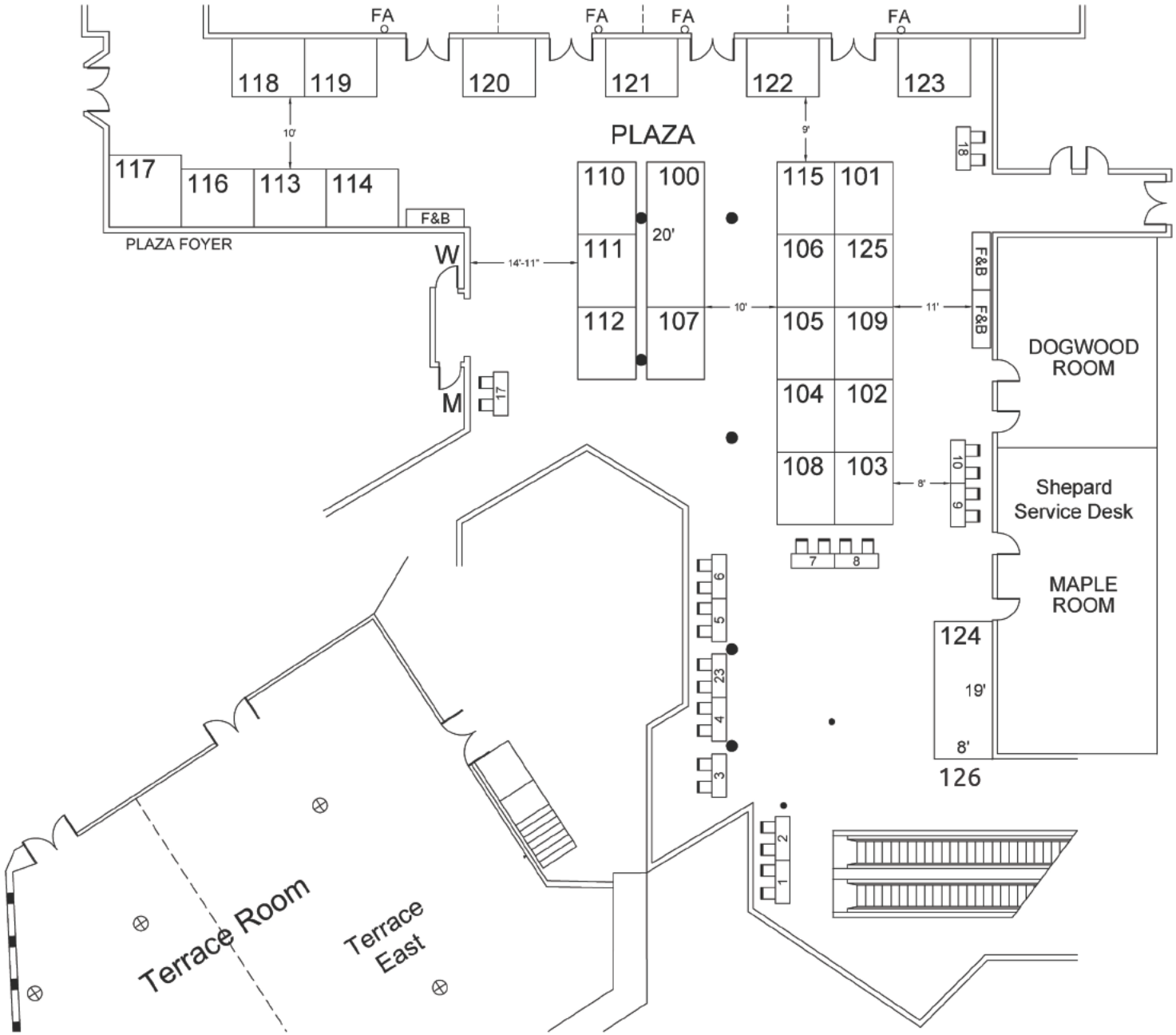


Drop off your business card in our raffle for a chance to win a flat screen TV!

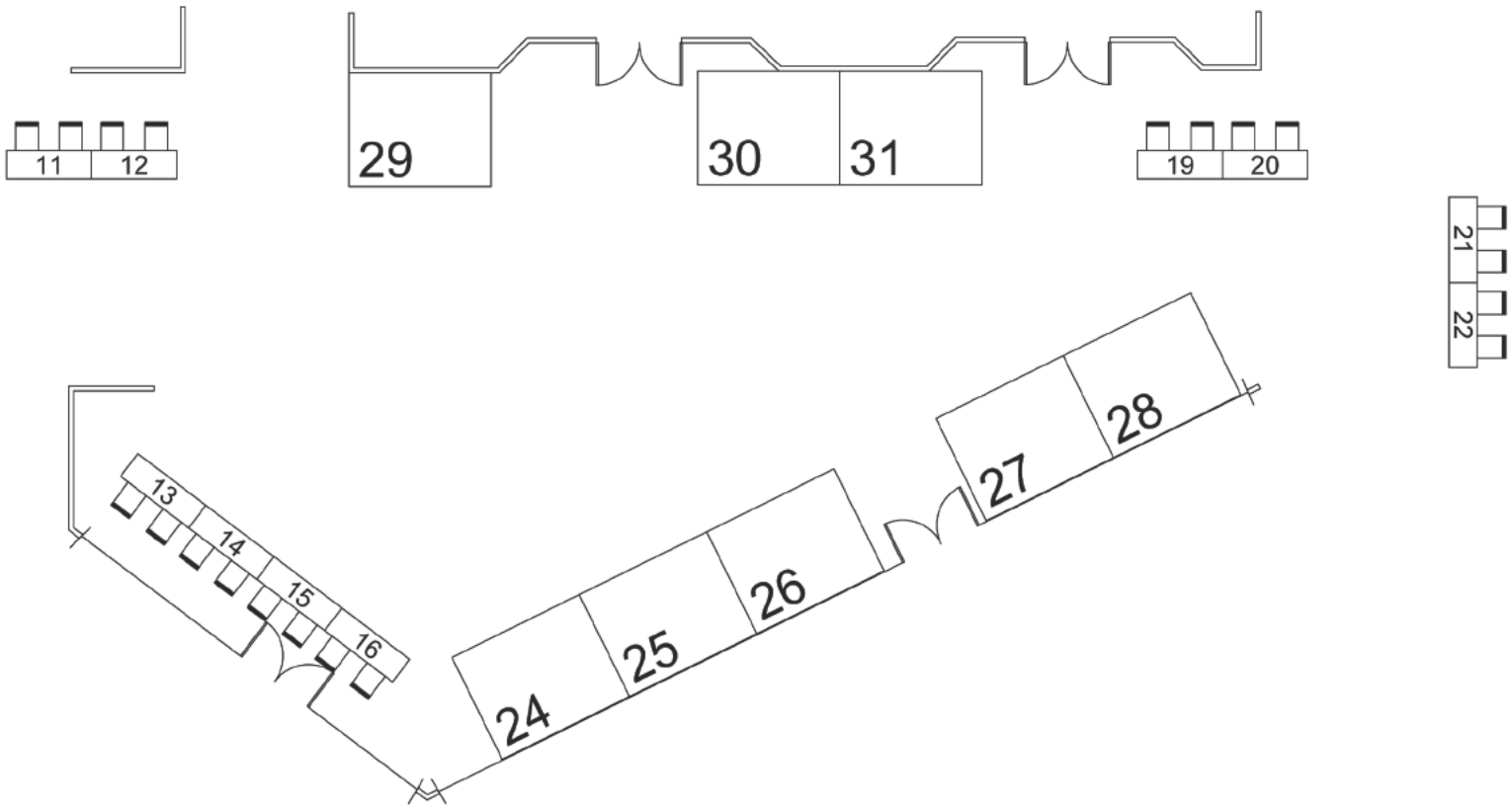
On-site Experts:
Michael Berndl mberndl@unchartedsoftware.com
Darryl Valinchus dvalinchus@unchartedsoftware.com

Learn more at www.geotime.com and request a 90-day trial.

2017 NFCA Annual Training Event
Hilton Alexandria Mark Center • Lower Level, Plaza Foyer



2017 NFCA Annual Training Event
Hilton Alexandria Mark Center • Lower Level, Plaza Foyer



CONNECTICUT ACADEMY OF SCIENCE AND ENGINEERING

CVISN E-SCREENING AND OVERWEIGHT SCREENING PILOT PROJECT

STUDY COMMITTEE MEETING

DATE/TIME: Wednesday, May 24, 2017
9:00 am to 12:00 am EST

LOCATION: CASE Offices, 805 Brook Street, Building 4-CERC, Rocky Hill

FOR TELECONFERENCE ACCESS:

Dial: 866-740-1260
Access: 5272161#

AGENDA

- **Welcome**
  Richard H. Strauss, Executive Director, CASE

- **Guest Presentation**
  Enrique Cramer, Business Development Director
  Intelligent Imaging Systems

- **CTDOT Study Contact Presentation**
  Brad Overturf, Transportation Supervising Engineer
  Bureau of Policy and Planning

- **Guest Presentation**
  University of Nevada, Reno – Department of Civil & Environmental Engineering
  - **Elie Y. Hajj**, Ph.D., Associate Professor & Associate Director of WRSC, Pavement Engineering & Science Program
  - **Raj Siddharthan**, Ph.D., P.E., Professor

- **Next Steps**

Upcoming Meeting Scheduled:
Wednesday, June 28, 2017, 9:00 am – 12:00 pm EST
CASE Offices, 805 Brook Street, Building 4-CERC, Rocky Hill, CT

To our valued customers,

As you may be aware, Neology has recently completed the acquisition of the ALPR and the electronic toll collection business from 3M's Transportation Safety Division. On behalf of all of the employees at the now larger Neology, we look forward to working with you. We are excited to bring an innovative spirit and the combined resources of our new larger company to our customers.

With the acquisition of the ALPR business, Neology is able to offer a full spectrum of mobile and fixed cameras, software, and services in automated license plate recognition throughout the U.S. as well as other key geographies worldwide.

Neology has brought back the PIPS Technology brand and our mission is to deliver on our brand promises by providing best in class ALPR recognition systems, solutions, and service to our customers. We also look forward to supporting our legacy 3M ALPR hardware and software and providing upgrades as needed to our innovative new product line.

As part of this transition, all Purchase Orders should be sent directly to Neology effective November 1, 2017. Purchase Orders and other documents may be sent to: orders@pipstechnology.com.

Thank you for your continued patronage and support. Should you have any questions please do not hesitate to contact one of our colleagues below or our Customer Service Center at 833-PIPS-LPR.

Sales and Service:
833 PIPS LPR (833 747 7577) ext. 1 for Sales, ext. 2 for Service.

John Tedona
201 841 6237
jtedona@neology.net

Louis Wershaw
562 843 1066
lwershaw@neology.net

Miranda Fischer
651-347-1401
mfischer@neology.net

Best Regards,

PIPS Technology, a Neology business

THE COMMONWEALTH OF MASSACHUSETTS
EXECUTIVE OFFICE OF PUBLIC SAFETY AND SECURITY
Department of Criminal Justice Information Services
200 Arlington Street, Suite 2200, Chelsea, Massachusetts 02150, MASS.GOV/CJIS
TEL: 617-660-4600 • TTY: 617-660-4606 • FAX: 617-660-4613

Deval L. Patrick, *Governor* | Andrea J. Cabral, *Secretary of Public Safety and Security* | James F. Slater, III, *Acting Commissioner*

EXECUTIVE OFFICE OF PUBLIC SAFETY AND SECURITY DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES AUTOMATIC LICENSE PLATE RECOGNITION SYSTEMS CENTRAL REPOSITORY COMPANION POLICY

PURPOSE

To establish guidelines and best practices for data use, maintenance, training, and data storage associated with the usage of the Commonwealth Criminal Justice Information Automatic License Plate Recognition Systems Central Repository (Central Repository) by Massachusetts law enforcement agencies.

OVERVIEW

An Automatic License Plate Recognition (ALPR) system is a computerized system that uses high-speed digital cameras combined with sophisticated computer algorithms capable of converting the images of license plates to electronically readable data. The ALPR system captures an infrared image of a license plate and converts it to a text file using Optical Character Recognition (OCR) technology. The technology also compares the digital images of license plates to lists of known plates of interest. Currently, the ALPR is being utilized by many law enforcement and criminal justice agencies in the Commonwealth, which maintain the captured information in a database.

The Central Repository is a centralized data warehouse that stores ALPR information contributed by law enforcement and public safety agencies from the agency's database. By allowing the agencies to share and access the stored information, local, state and federal law enforcement agencies are provided accurate information to be used for official and legitimate law enforcement operations and public safety purposes. Guidelines for submission and retrieval of license plate data for all participating departments are included in the Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy of the Massachusetts Department of Criminal Justice Information Services (DCJIS), which is incorporated by reference, and this ALPR Central Repository Companion Policy. ALPR systems are dependent upon the networking system of Commonwealth's Criminal Justice Information System (CJIS) and all participating agencies and users agree to the terms of these policies.

DCJIS Enhancing Public Safety Through Information Exchange

POLICY

It is the policy of the DCJIS to utilize the technology only in furtherance of official and legitimate law enforcement operations and public safety. Recognizing privacy implications, it is further the policy of DCJIS to ensure the protection of data. Thus, all users of the Central Repository are expected to abide by the guidelines set forth herein when using the Central Repository.

ACRONYMS AND DEFINITIONS

Agency ALPR Administrator: An employee of a Participating Agency designated by that agency to be responsible for the management of its authorized users and the user accounts at the Participating Agency.

Authorized User: An individual designated by a law enforcement agency and properly trained in the use and operational protocols of the ALPR. Only authorized employees who have an approved login and password will be allowed to access or use information in the Central Repository.

Contributing Agency: An agency that contributes ALPR data to the Central Repository.

Non-Contributing Agency: An agency that may access, but does not contribute data to, a data application or system maintained or operated within the DCJIS network or system.

Participating Agency: Either a contributing or non-contributing party that utilizes the Central Repository.

Source Agency: The agency that originally recorded and contributed data to a data application or system maintained or operated within the DCJIS network or system.

PROCEDURES

1. Standard of Use

Central Repository ALPR data shall be accessed and used only for official and legitimate law enforcement operations and public safety and may only be used based on specific and articulable facts of a concern for safety, wrongdoing, criminal investigations, Department-related civil investigations, or pursuant to a court order.

Searches of historical Central Repository ALPR data shall be done in accordance with this policy.

Only users who have been designated by their law enforcement department and properly trained in the use and operational protocols of the ALPR systems shall be permitted to use the Central Repository. DCJIS administrators shall ensure that any changes in hardware, software or law are communicated to all participants. Only authorized employees who have an approved login and password (Central Repository Authorized Users) will be allowed to access or use information in the Central Repository.

When a enforcement action, investigation, or prosecution results from the Repository ALPR data, the information contained in it will be preserved by the agency accessing the information.

Requests for searches of Central Repository ALPR data may be made by authorized members of the Contributing Party or Non-Contributing party subject to the provisions of this policy.

2. Login Application Process

   a) Each Contributing and Non-contributing Party shall designate an Agency ALPR administrator to be responsible for management of user accounts at that agency. All authorized users shall be limited to current employees who are legally authorized to review criminal justice information for crime prevention and detection purposes. Each potential user shall submit a request for a login and password to the Agency ALPR Administrator. The Agency ALPR Administrator shall have discretion to deny or revoke individual access.

3. Login Assignment

   a) Each Authorized User will be issued a user login and a default password by the Agency ALPR Administrator. Upon logging into the Repository for the first time, each Authorized User shall change the default password to another DCJIS-compliant password.

   b) Each Agency ALPR Administrator is responsible for the timely removal of any login accounts as Authorized Users leave their agency.

   c) An Authorized User shall not access the Central Repository by using a name and 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.

4. ALPR Central Repository Data Query Logs

   a) An automated log will be maintained for each transaction, which will include the name of the individual accessing the data, along with the date and time of access.

b) Requests to review stored ALPR data and search results will be recorded and maintained in appropriate case files.

c) ALPR Data Query Logs shall be maintained and secured.

d) Audits of the ALPR systems and the central repository shall be conducted by the DCJIS.

5. ALPR Data Sharing and Dissemination

a) Each Contributing Agency authorizes the release of its information as outlined in this Policy to any other criminal justice agency that may participate in the Central Repository in the future.

b) A Contributing Party that does not want certain information from its ALPR system to be shared is responsible for filtering out such information before entering it into the Central Repository.

c) The information contributed to the Central Repository is limited to ALPR data.

d) Central Repository ALPR data can be accessed, retrieved, or shared for official and legitimate law enforcement operations or public safety purposes only.

6. Ownership of Data

a) Each Contributing Party will retain sole responsibility, ownership, management control, and disposition over the information it contributes or allows access to. All system entries will be identifiable to the Contributing Party, and the content of the contributed information remains the sole responsibility of the Contributing Party and is under that Contributing Party's management control.

b) It shall be the responsibility of the party requesting or using the data to confirm the accuracy of the information with the Source Agency before taking any enforcement-related action.

7. Retention of Data

a) Data from field ALPRs will be transferred/uploaded to the Department's server at a time to be determined by the Agency ALPR Administrator.

b) ALPR data shall be stored in the Central Repository for a period of one year except in the following circumstances:

i) Alert data associated with an enforcement action, investigation, or prosecution shall be maintained for one year or until a final disposition has been reached in the particular case, whichever is longer.

ii) Alert data associated with an arrest will be maintained in the criminal case file and retained for the maximum period of time associated with such record.

iii) Alert data associated with criminal investigations will be maintained in the criminal case file and retained for the maximum period associated with such record.

iv) If it is reasonable to believe and the ALPR data will become evidence in a criminal or civil action, the record will be maintained until it is no longer reasonable to believe it will become evidence in a criminal or civil action.

v) Whenever otherwise directed by the ALPR Administrator.

CONFIDENTIALITY OF INFORMATION

Information in the Central 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, otherwise, the information shall be kept confidential.

ACKNOWLEDGEMENT OF TERMS AND CONDITIONS OF USE

The Agency ALPR Administrator shall provide a copy of the terms and conditions of the Massachusetts Public Safety Information Sharing Global Policy and this ALPR Central Repository Companion System Policy to all Authorized Users when they are issued a login ID for the system. Each Authorized User shall sign an acknowledgement stating, "I have received a copy of the terms and conditions of usage of the Central Repository. I agree to comply with the terms and conditions and I understand that any violation of the terms and conditions may lead to disciplinary action and/or criminal prosecution." The Agency ALPR Administrator shall maintain the signed acknowledgements at all times.

POLICY REVIEW

The Commissioner of the Department of Criminal Justice Information Services is responsible for the annual review of this policy.

Watch Office Job Aid

ALPR HotLists

July 2017

Overview

License plates of interest can be added to the Hotlist in the 3M BOSS Automated License Plate Recognition (ALPR) system. When a Hotlist plate is read by an ALPR camera, an email will send to the requesting officer. Officers can determine if they want the passing ALPR system to be alerted as well.

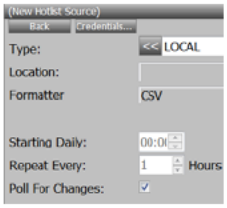


Fusion's 3M software is located at M:\SA Client 3.2.0

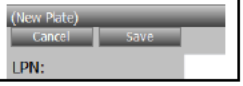
Steps

Entering a license plate into the 3M Boss HotList involves two steps: Create a Case, and Enter the Plates. The process is shown below. For brevity, some steps have been grouped (i.e. Deployment has steps A, B, C).

Create a Case

Step	Action
1	**Click** Admin [Admin] and then **Click** Hotlists (left). The Hotlist is displayed. **Click** New [New] (bottom). The Hotlist entry page is displayed.
2	Select or Enter the following values: Hotlist Name: *(*i.e. *Agency – Case Number, Agency – Plate)* Description: *(Officer name, plate, etc.)* Deployment: A. **Click** Select, B. **Check** ALL boxes, C. **Click** Save
3	**Click** Source and Select or Enter the following values Type: *Local (default)* Location: *Leave blank* Formatter: A. **Click** Select, B. **Select** CSV, C. **Click** Save Poll for changes: **Check** the box **Click** Back 
4	**Click** Advanced and enter the following values Covert: If checked, passing ALPRs will NOT be alerted Notify Email: Enter emails separated by commas Expires: Three months from entry date  **Click** Back and then **Click** Save **Click** Save **Click Yes** on the "Source file name" error message

Enter the Plates

Step	Action
1.	**Click** on the Hotlist item in the list
2.	**Click** Plates [Plates] (bottom) and then **Click New**
3.	**Enter** the plate number in LPN (no state) **Click** Save (repeat as necessary) 

THE COMMONWEALTH OF MASSACHUSETTS
EXECUTIVE OFFICE OF PUBLIC SAFETY AND SECURITY
Department of Criminal Justice Information Services
200 Arlington Street, Suite 2200, Chelsea, Massachusetts 02150, MASS.GOV/CJIS
TEL: 617-660-4600 • TTY: 617-660-4606 • FAX: 617-660-4613

Deval L. Patrick, *Governor* | Andrea J. Cabral, *Secretary of Public Safety and Security* | James F. Slater, III, *Acting Commissioner*

MODEL POLICY FOR LAW ENFORCEMENT AGENCIES - AUTOMATIC LICENSE PLATE RECOGNITION (ALPR) SYSTEMS

Policymakers are encouraged to customize this document for their agency giving consideration to personnel assignments, resources, infrastructure, and community served.

I. PURPOSE

The purpose of this Policy is to establish guidelines and procedures for the proper use and application of automatic license plate recognition (ALPR) systems, the management of the data, and the maintenance of the equipment.

II. POLICY

The availability and use of ALPR systems have provided many opportunities for the enhancement of law enforcement agencies' productivity, effectiveness, and protection of public and officer safety. It is the policy of this Department to only utilize the technology in furtherance of official and legitimate law enforcement operations and public safety. All members of this Department are expected to abide by the guidelines set forth herein when using ALPR systems.

III. ACRONYMS AND DEFINITIONS

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: Automatic License Plate Recognition. 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.

ALPR data: Scan files, alert data, and any other documents or data generated by, or obtained thorough, utilization of the ALPR system.

ALPR Data Query Logs: A record of a search or query of ALPR data.

ALPR system: The ALPR camera and all associated equipment and databases.

Department: Town/City Police Department.

Fixed ALPR system: ALPR cameras that are permanently affixed to a structure, such as a pole, a traffic barrier, or a bridge.

GPS: Global positioning system.

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, 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.

Mobile ALPR system: ALPR cameras that are affixed, either permanently (hardwired) or temporarily (e.g., magnet-mounted), to a law enforcement vehicle for mobile deployment.

OCR: Optical Character Recognition. The technology that supports the automated reading and digitizing of images of license plates that are captured by the ALPR system.

Portable ALPR system: ALPR cameras that are transportable and can be moved and deployed in a variety of venues as needed, such as a traffic barrel or speed radar sign.

IV. PROCEDURES

A. General

ALPR systems and associated equipment and databases are the property of this Department and authorized for official use only. Misuse of this equipment and associated databases or data may be subject to sanctions and/or disciplinary actions, as determined by the rules and regulations of the Department.

B. Administration

1. The Department shall designate an employee(s) in a command position with administrative oversight as the ALPR Administrator for the ALPR system deployment, operations, and maintenance. The ALPR Administrator or a designee shall be responsible for the following:

(a) Establishing protocols for access, collection, storage, and retention of ALPR data and associated media files;

(b) Establishing protocols to preserve and document ALPR reads and "alerts" or "hits" that are acted on in the field or associated with investigations or prosecutions;

(c) Establishing protocols to establish and ensure the security and integrity of data captured, stored, and/or retained by the ALPR system;

(d) Ensuring the proper selection of the personnel approved to operate the ALPR system and maintaining an adequate number of trained and authorized users;

(e) Maintaining records identifying approved ALPR deployments and documenting their results, including appropriate documentation of significant incidents and arrests that are related to ALPR usage;

(f) Authorizing any requests for ALPR systems use or data access according to the policies and guidelines of this agency;

(g) Managing and securing the data, including requests for searches of the ALPR data, hot lists, and backing up the ALPR data; and

(h) Ensuring that designated, trained personnel check equipment on a regular basis to ensure functionality and camera alignment and removing from service any equipment that falls outside expected functionality until deficiencies have been corrected.

2. ALPR systems repairs (hardware or software) shall be made by Department-authorized sources.

C. Automatic License Plate Recognition System Usage

1. ALPR systems and information shall be accessed and used only for official and legitimate law enforcement operations and public safety related purposes, and may only be used based on specific and articulable facts of a concern for safety, wrongdoing, criminal investigations, Department-related civil investigations, or pursuant to a court order.

2. Searches of historical ALPR data shall be done in accordance with established departmental policies and procedures.

3. Only users who have been designated by the ALPR Administrator and properly trained in the use and operational protocols of the ALPR system shall be permitted to use the system. Only those users with an approved login and password will be allowed access to the ALPR system.

4. The agency's ALPR Administrator shall ensure that any changes in hardware, software, policy, or law are the subject of continuing in-service training or bulletins.

5. The use of ALPR technology must be approved by the agency head or designee.

6. When an enforcement action, investigation, or prosecution results from an ALPR hit, the hit will be preserved.

7. ALPR hot lists and data gathered by departmental ALPRs will be maintained securely.

8. Requests for searches of ALPR data to the ALPR Administrator may be made by members of this Department or by other law enforcement agencies subject to the provisions of this Policy.

D. Operational Procedures

1. At the start of each shift, users shall ensure that the ALPR system has been updated with the most current hot lists available.

2. At the beginning of each tour of duty, users should verify the aim of the ALPR camera(s) to ensure it is focused on the correct lanes of traffic.

3. ALPR equipment should be cleaned and maintained according to the manufacturer's recommendations.

4. Any damage to ALPR systems will be reported immediately according to the Department's established policy and procedures related to the loss of, or damage to, the Department's equipment.

5. When not in use, ALPR-equipped vehicles should be secured. Users on extended leave should remove the ALPR equipment and secure it within the trunk or other secure location.

6. The user shall notify the ALPR Administrator of any malfunction of the ALPR.

E. Manual Entry of Data

1. Users may become aware of additional potential license plate numbers of interest and may request those license plate numbers be entered into the Department hot list. License plates may be entered only when directed or authorized by *[specify command position]* and only for official and legitimate law enforcement or public safety operations.

2. A second party check must be conducted on all manual entries.

3. Manual entries may include, but should not be limited to, an AMBER Alert, Missing Child Alert, Missing College Student Bulletin, Be On Look Out (BOLO), Attempt To Locate (ATL), or Wanted or Missing Person broadcast or bulletin in which a license plate number is included. Such manual entries must be manually updated when the information changes or is no longer current.

4. Whenever a plate is manually entered into the ALPR system, the officer shall document the reason.

F. ALPR Alerts/Hits

Prior to initiation of a stop based on a hit or alert:

(a) Users shall 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 issuance.

(b) Users shall verify the current status of the plate through the Commonwealth's Criminal Justice Information System (CJIS), National Crime Information Center (NCIC), Department's Records Management System (RMS), or other appropriate source of data prior to a stop when circumstances allow or as soon as practicable.

V. INFORMATION MANAGEMENT

A. ALPR Data Query Logs

1. An automated log will be maintained for each transaction that will include the name of the individual accessing the data, along with the date and time of access.

2. Requests to review stored ALPR data and search results will be recorded and maintained in appropriate case files as determined by the rules and regulations of the Department.

3. ALPR Data Query Logs shall be maintained and secured.

4. Audits shall be conducted at the discretion of the Department head.

B. ALPR Data Sharing and Dissemination

1. ALPR data can be accessed, retrieved, or shared for official and legitimate law enforcement operations or public safety purposes only.

2. Dissemination of ALPR data outside the Department shall be documented in a secondary dissemination log, as determined by the rules and regulations of the Department.

3. Information sharing among law enforcement agencies, other than the DCJIS, should be governed by departmental policies or memoranda of understanding.

C. Retention

1. Data from ALPRs will be transferred/uploaded to the Department's server at a time to be determined by the ALPR Administrator. Data captured by the ALPR will be purged once the upload to the Department sever is complete.

2. All ALPR data may be stored in the Department's server for a period of one year, except that data may be stored for longer than one year in the following circumstances:

(a) Alert data associated with an enforcement action, investigation, or prosecution shall be maintained until a final disposition has been reached in the particular case.

(b) Alert data associated with an arrest will be maintained in the criminal case file and retained for the maximum period of time associated with such record.

(c) Alert data associated with criminal investigations will be maintained in the criminal case file and retained for the maximum period associated with such record.

(d) If it is reasonable to believe that the ALPR data will be used as evidence in a criminal or civil action, the record will be maintained until it is no longer reasonable to believe it will be used as evidence in a criminal or civil action.

(e) Whenever otherwise directed by the ALPR Administrator.

VI. STATE CENTRAL REPOSITORY

[For EOPSS Highway Safety Division grantees:]

1. The Department has procured the ALPR systems under a grant program of the Executive Office of Public Safety and Security's Highway Safety Division. As a grantee, the Department has agreed to electronically submit captured ALPR data to the state repository maintained by the Department of Criminal Justice Information Services (DCJIS) at the Commonwealth's Public Safety Data Center. Captured ALPR data will be made available to local, state, and national law enforcement as needed to support official law enforcement operations. Guidelines for submission and retrieval of license plate data for all participating departments are included in the Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy of the DCJIS and the ALPR Central Repository Companion Policy attached to this directive. This Department and its users agree to the terms of these policies.

[For others:]

1. To enhance local and statewide law enforcement efforts, the Department has agreed to electronically submit captured ALPR data to the state repository maintained by the Department of Criminal Justice Information Services (DCJIS) at the Commonwealth's Public Safety Data Center. Captured ALPR data will be made available to local, state, and national law enforcement as needed to support official law enforcement operations. Guidelines for submission and retrieval of license plate data for all participating departments are included in the Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy of the DCJIS and the ALPR Central Repository Companion Policy attached to this Special Order. This Department and its users agree to the terms of these policies.

VII . POLICY REVIEW

1. The ALPR Administrator is responsible for the annual review of this Policy and the policies and procedures contained herein and for making recommendations to the Department head for any necessary amendments. This is a new technology and it may raise both legal and technological issues. As use of the technology progresses, the Department will continue to monitor and assess the appropriateness of this Policy.

Automated License Plate Reader

MSP DEPLOYMENT 2/15/13

DEPLOYMENT

- Initial Deployment 6/2009. One cruiser [redacted] -CAT as a result of an EOPSS grant.
- Critical Infrastructure Grant 2/201[redacted] - [redacted] cruisers outfitted w/ [redacted].
- Troop E deploys two mobile units to determine future utilization of mobile and fixed cameras.

Line Up



Light Bar Mount



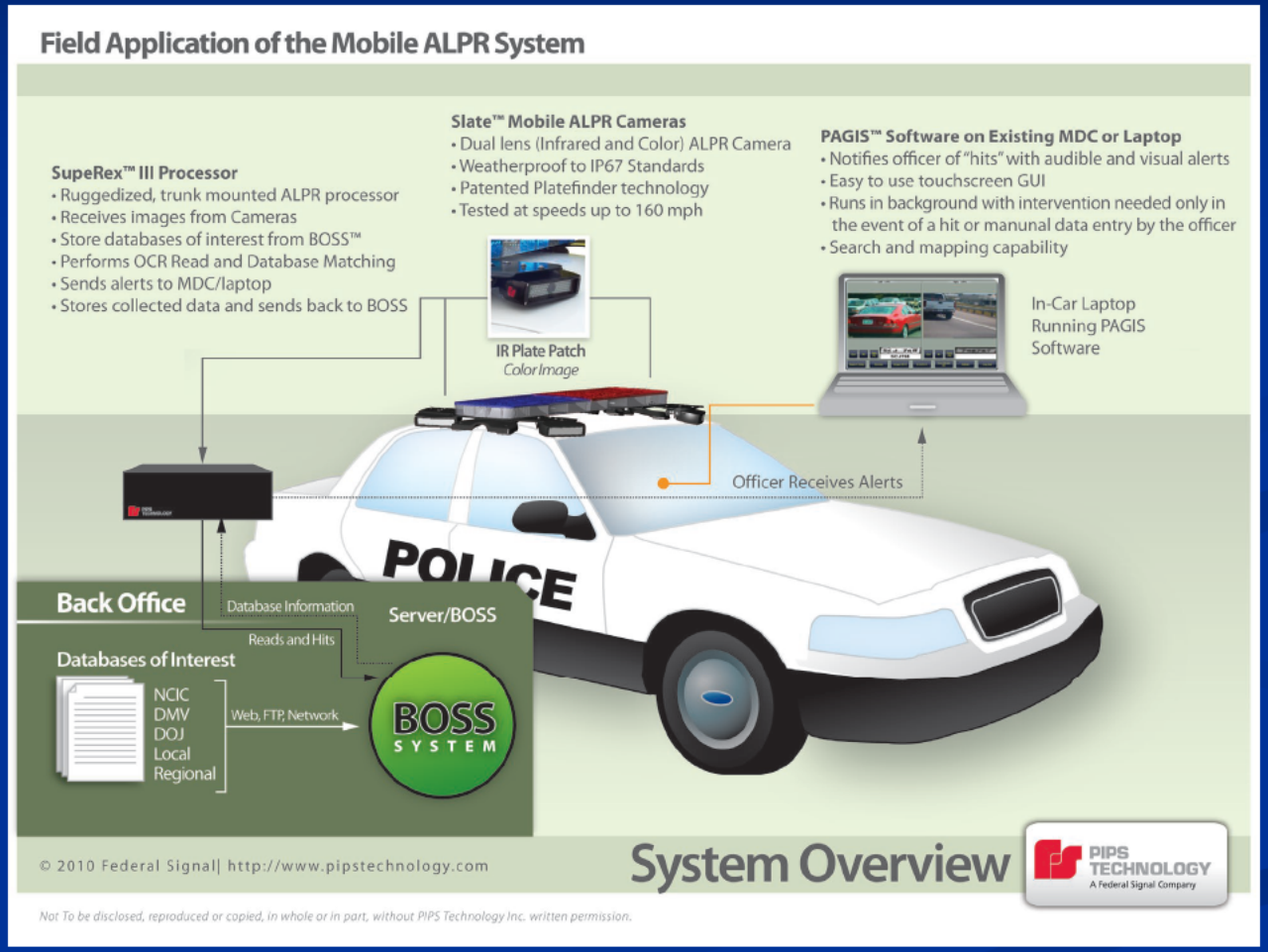
Trunk Mount



Covert Grille Installation



System Overview



3M ALPR Expertise and Design Options

- 27 years of camera design experience
- 18 years of ALPR camera experience
- Integrated Color and Infrared as PIPS Standard
- Different Wavelength LED's for different plate populations
- PIPS is the pioneer
  - First to offer standard dual lens
  - First to offer integrated processor
  - Several patents, others pending

PAGIS Cruiser software

Mobile ALPR System for Law Enforcement

Parking Applications

KIS – Simple is Good

Displays Camera Feeds

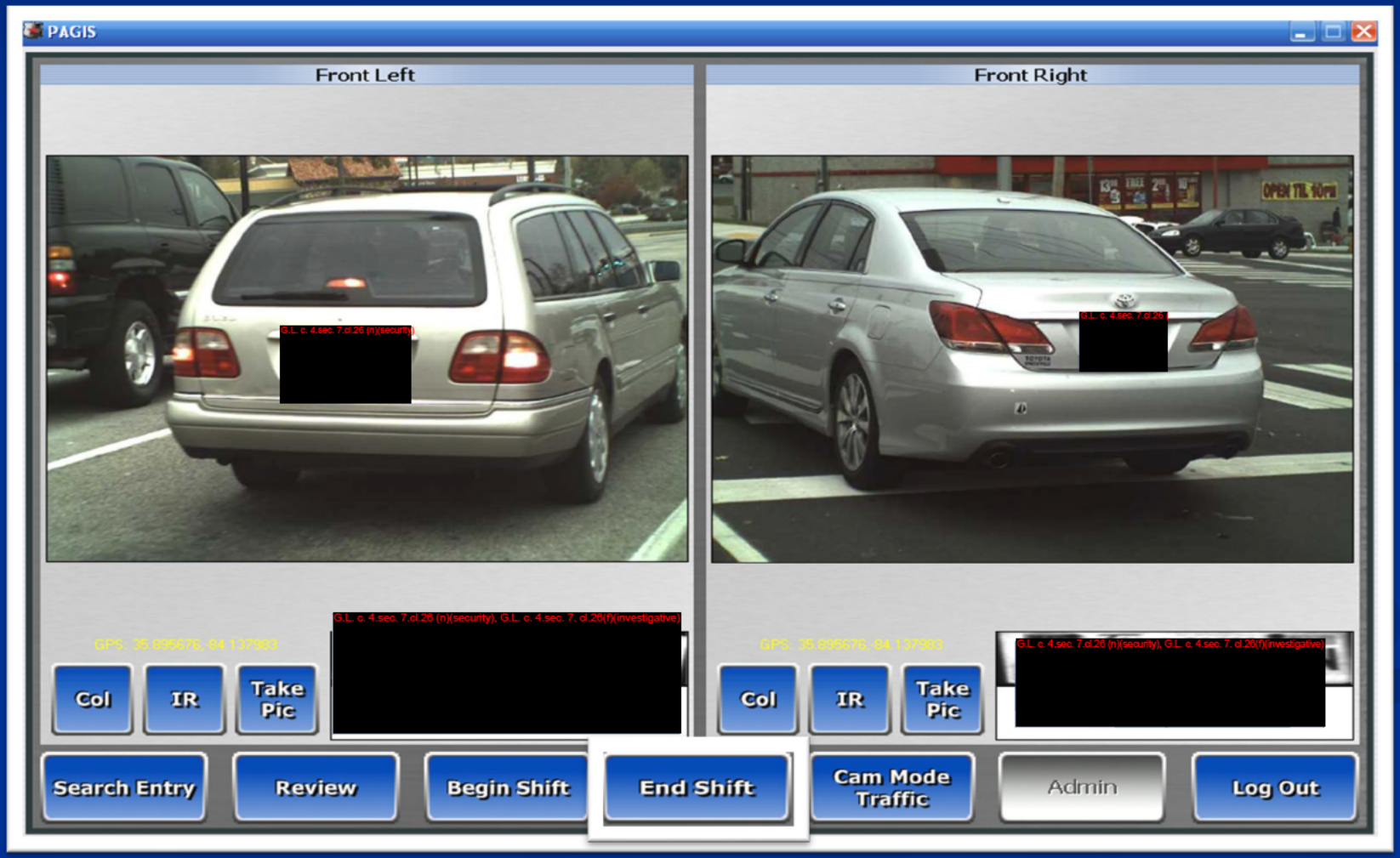
Matching Against Multiple Databases – Alerts

- NCIC Stolen
- Wanted Felons
- AMBER Alerts
- Unregistered Vehicles
- DUI Probation
- Others

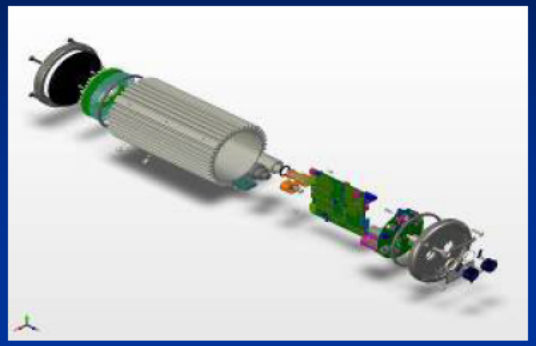
Search or input scanned plates



PAGIS – 7 Primary Buttons – Very Easy to Use



How ALPR Works



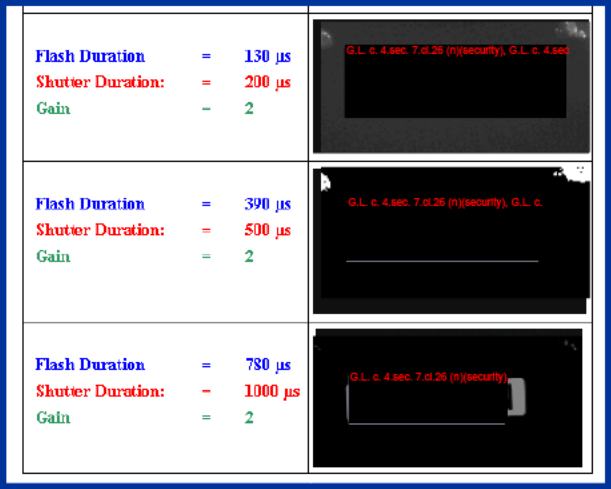
Advanced Camera Design



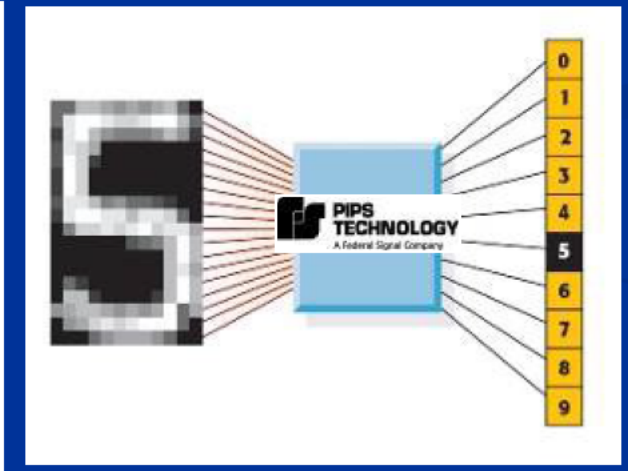
Infrared Illumination



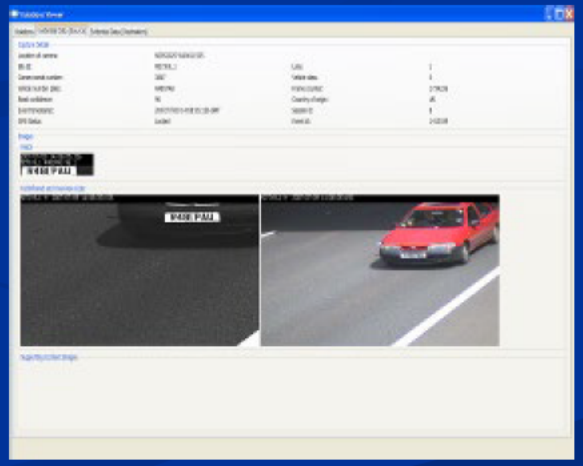
Plate Detection



TripleFlash Image Capture

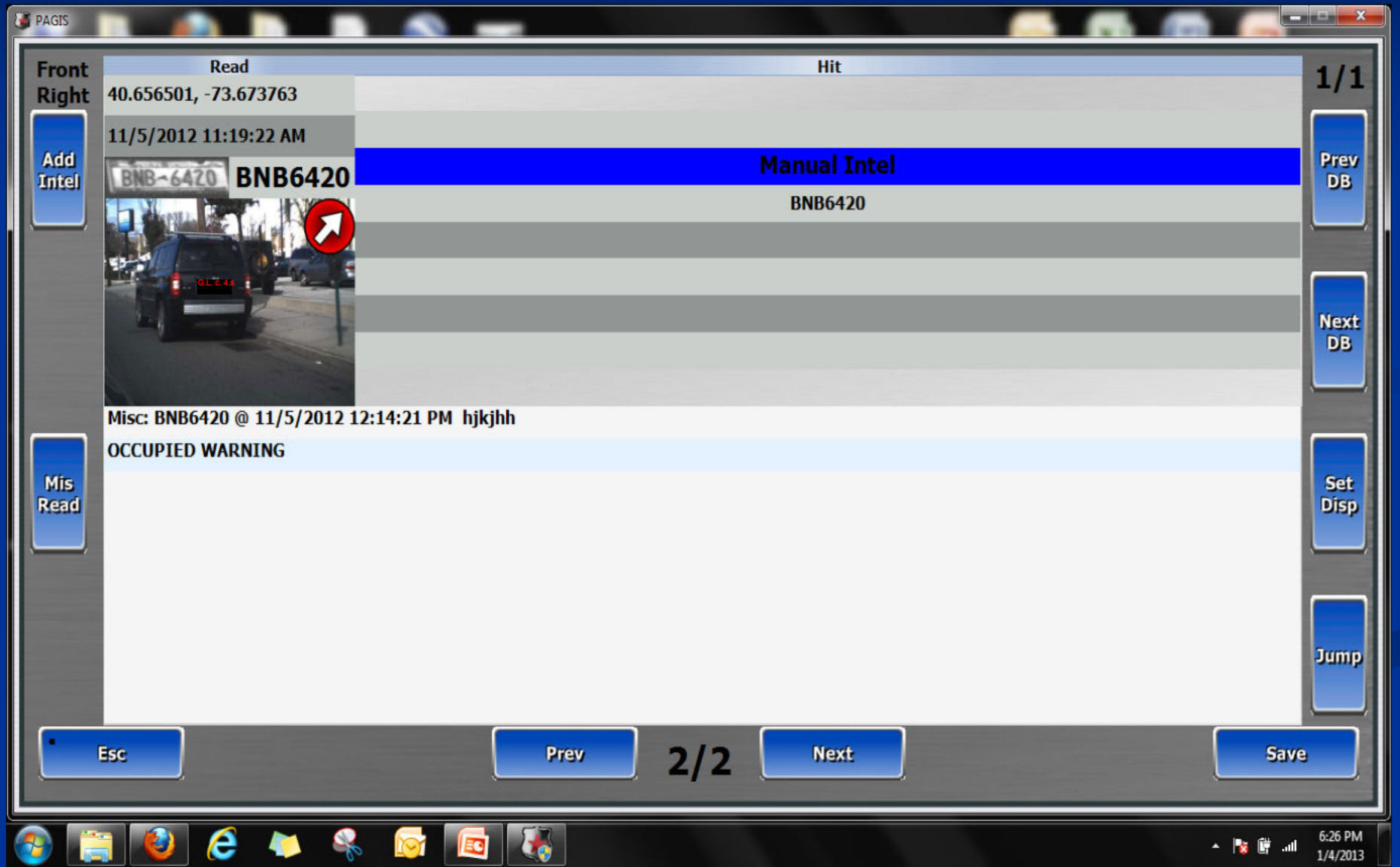


Optical Character Recognition

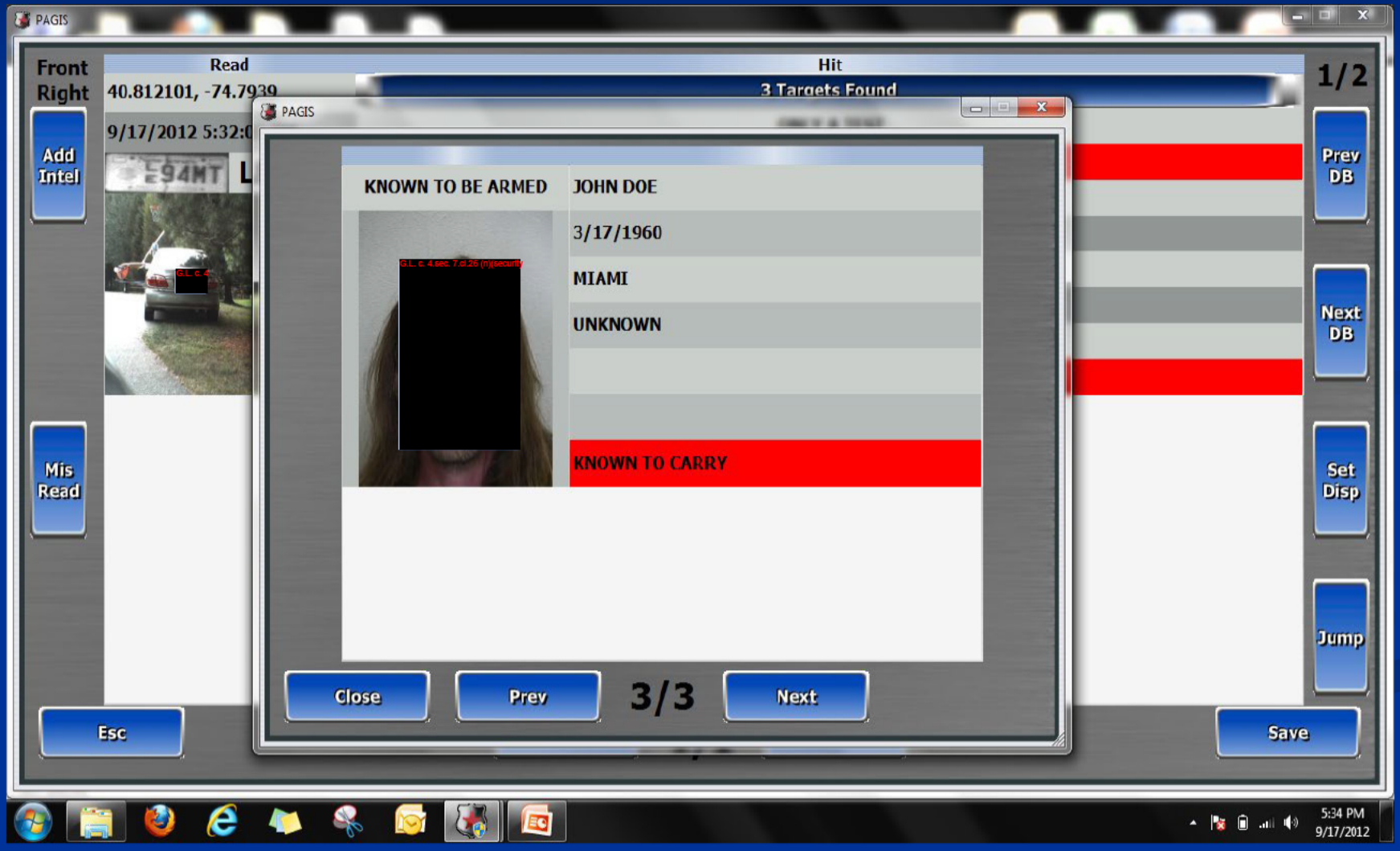


Package Data for Software Use

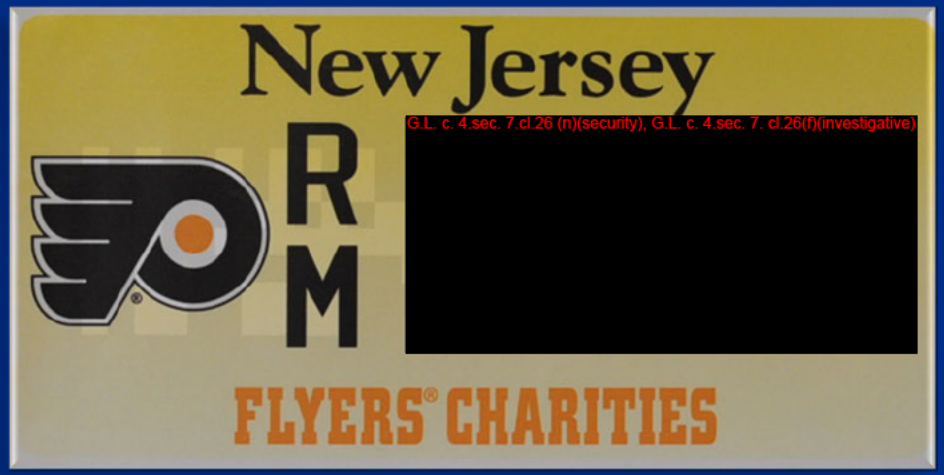
Hit Alert


PAGIS
Front Right
Read
Hit
1/1
40.656501, -73.673763
11/5/2012 11:19:22 AM
BNB6420
Manual Intel
BNB6420
Add Intel
Prev DB
Next DB
Mis Read
Set Disp
Jump
Misc: BNB6420 @ 11/5/2012 12:14:21 PM hjkjhh
OCCUPIED WARNING
Esc
Prev
2/2
Next
Save
6:26 PM
1/4/2013

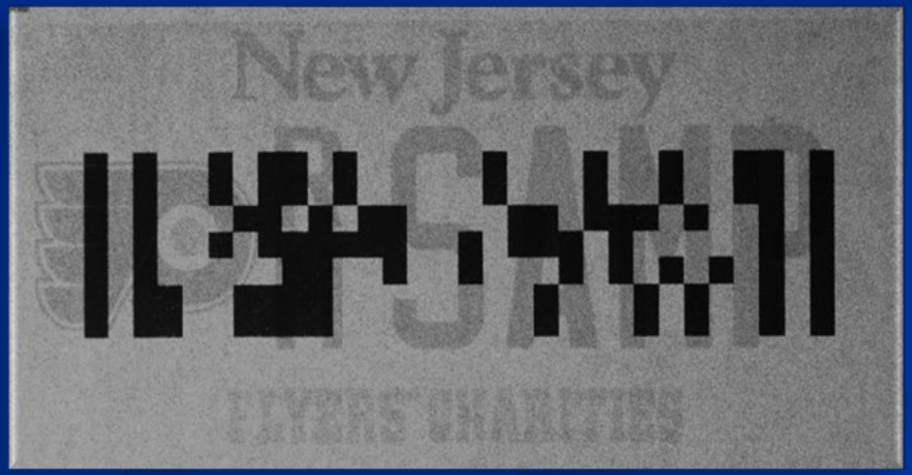
Hotlist Match – Targets



Machine Readable License Plate Barcode Concept/ Future Mass Plates



Visible light



Infrared (IR) light

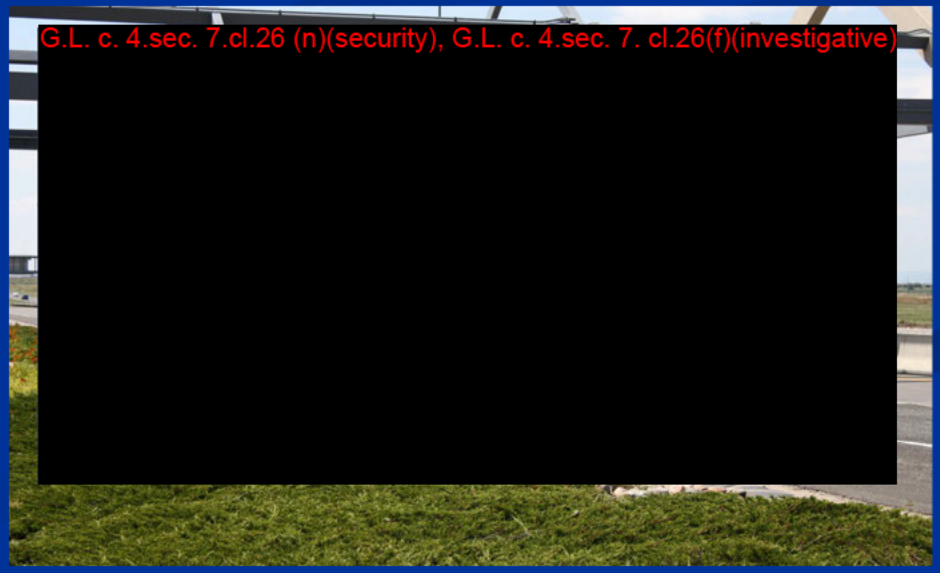
Joint Patent between legacy PIPS and 3M
Full Field Barcode Eliminates Interference from Plate Frames
Provides Highest Degree of Accuracy
Provides More Information to Officers

ALPR Fixed Cameras



Chicago O'Hare Intl Airport

RTE [redacted] Colorado



BOSS 3.0 Inter-Agency Data Sharing Connection GUIDE

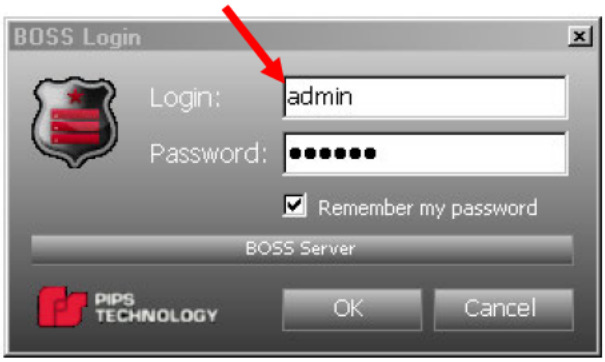
Your agency's BOSS server can share data with another agency's BOSS server as long as the two servers can communicate with each other over port 23032. The network routes, firewall settings, etc. to allow for this connection are the responsibility of the connecting agency's IT departments.

This step by step guide describes:

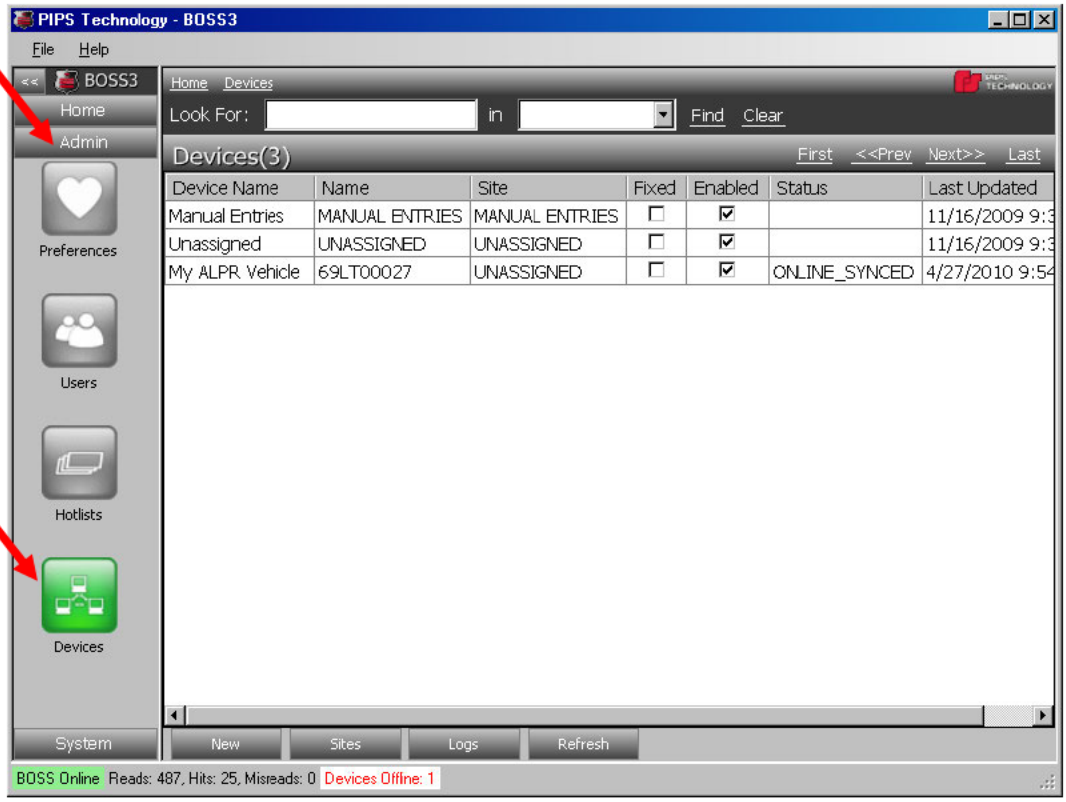
1. How to create a new Remote Site - Page 3.
2. How to add IP address, Login name, and Password to the new Remote Site - Pages 3
3. How to create a new Remote Group - Page 5
4. How to add a new Role to the Remote Group - Page 6
5. How to create a new User account for new Remote Group - Page 8
6. How to give Permissions to the new Remote Group - Page 9
7. Test the connection to the new Remote Site – Page 10

Login to BOSS as an administrator:

1. Login to BOSS as an administrator

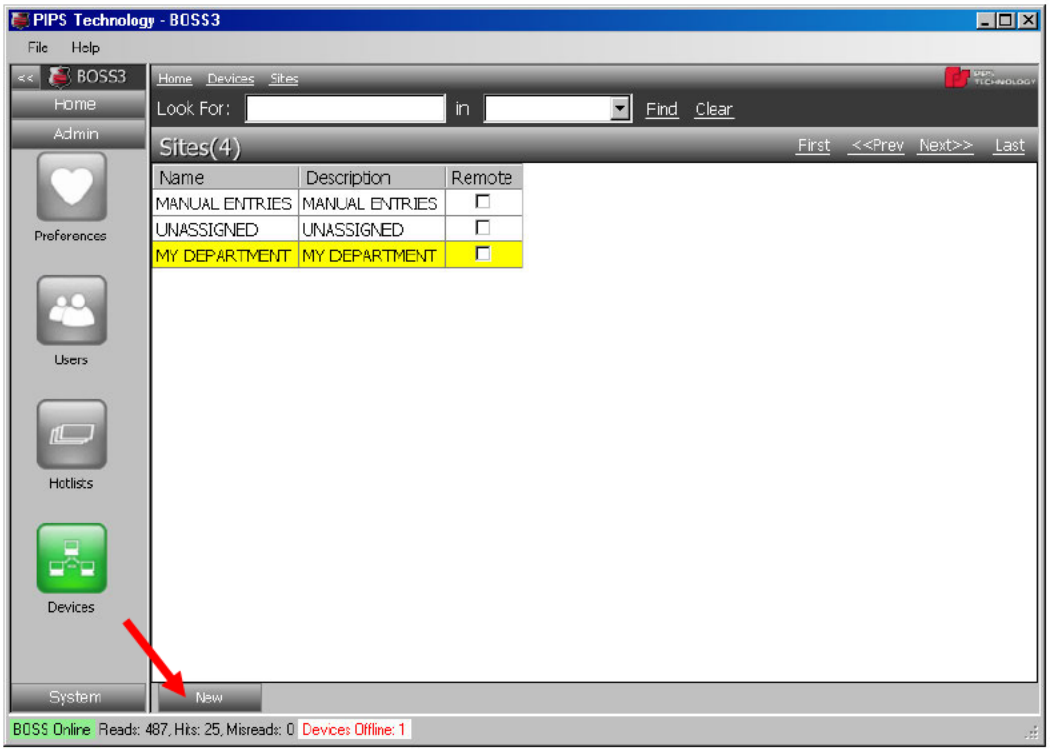


2. Click “Admin”, then “Devices” (The site to be added will be the other agency’s BOSS server)

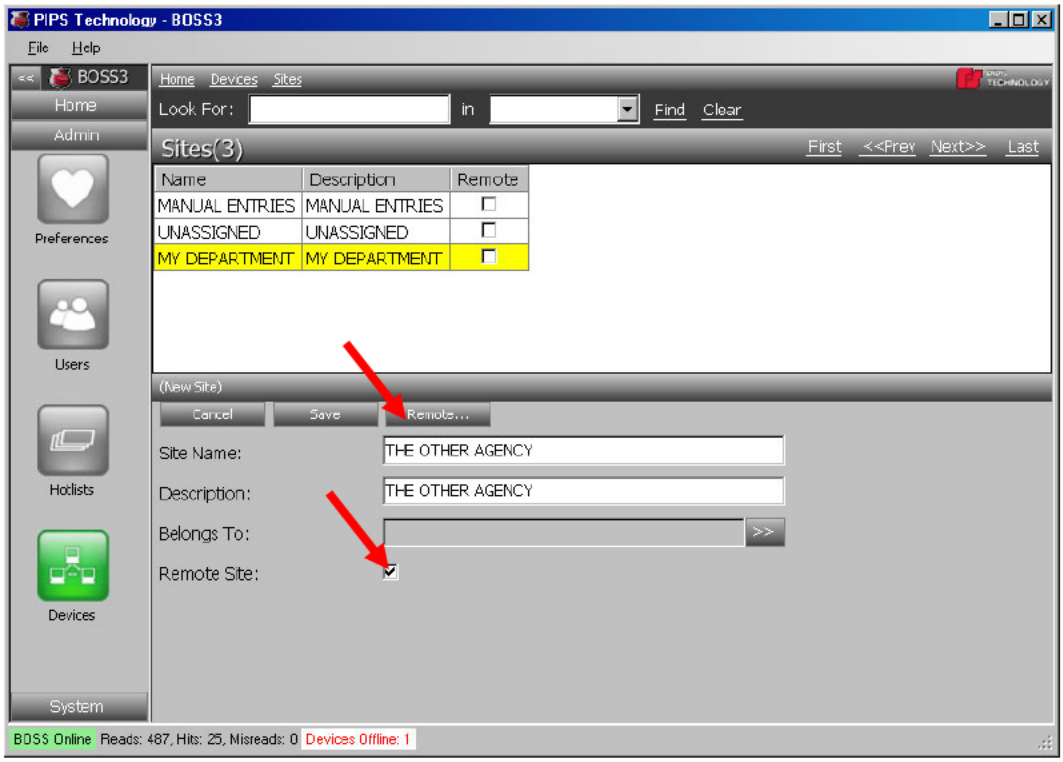


Create a new Remote Site

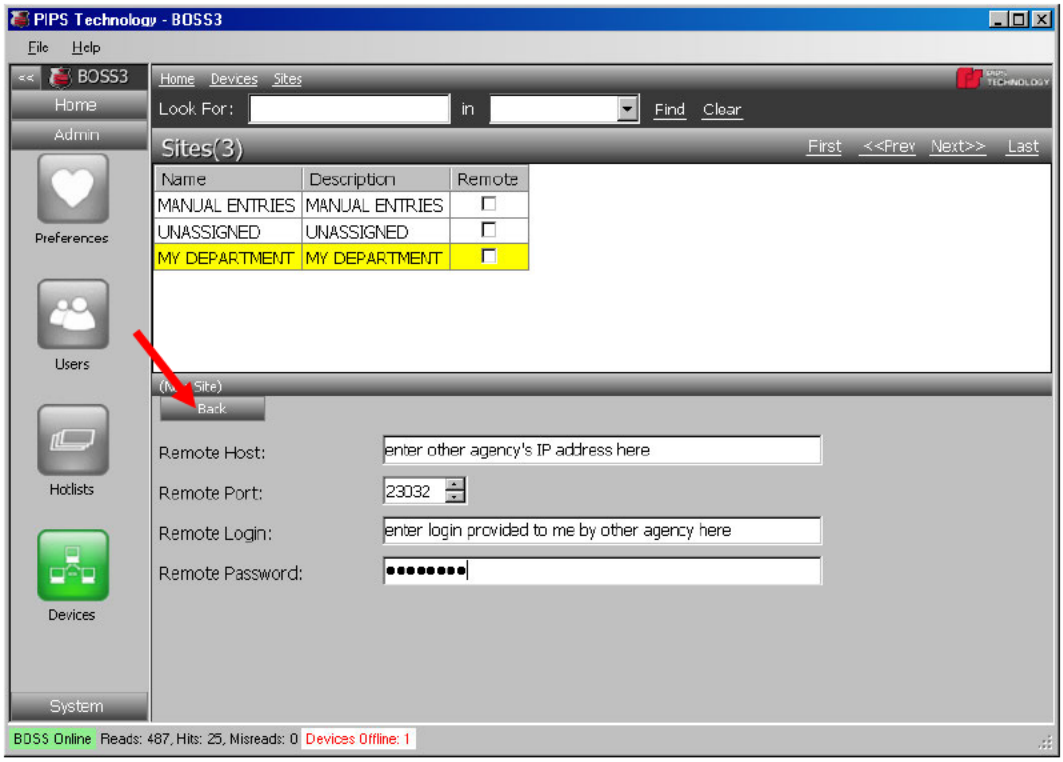
3. Click “New” to add a new remote site:



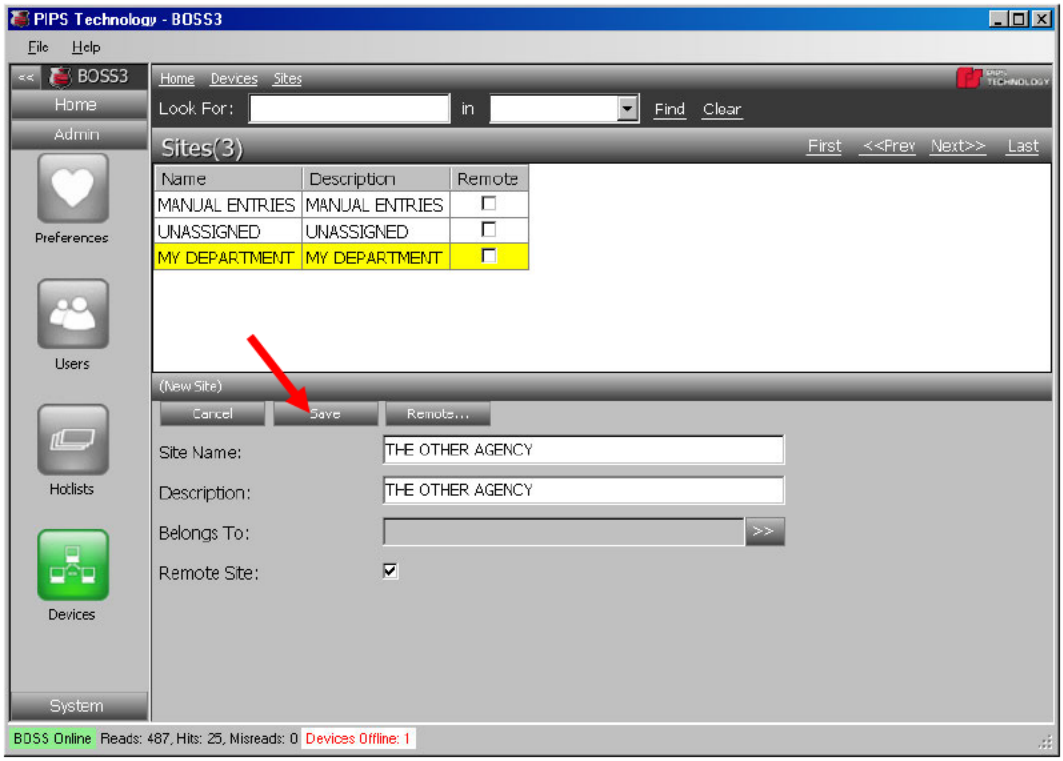
4. Enter info for the other agency’s site. Check the “Remote Site” box, then click the “**Remote…**” button:



5. Enter the IP address and login/password provided to you by the other agency. Hit “Back”.

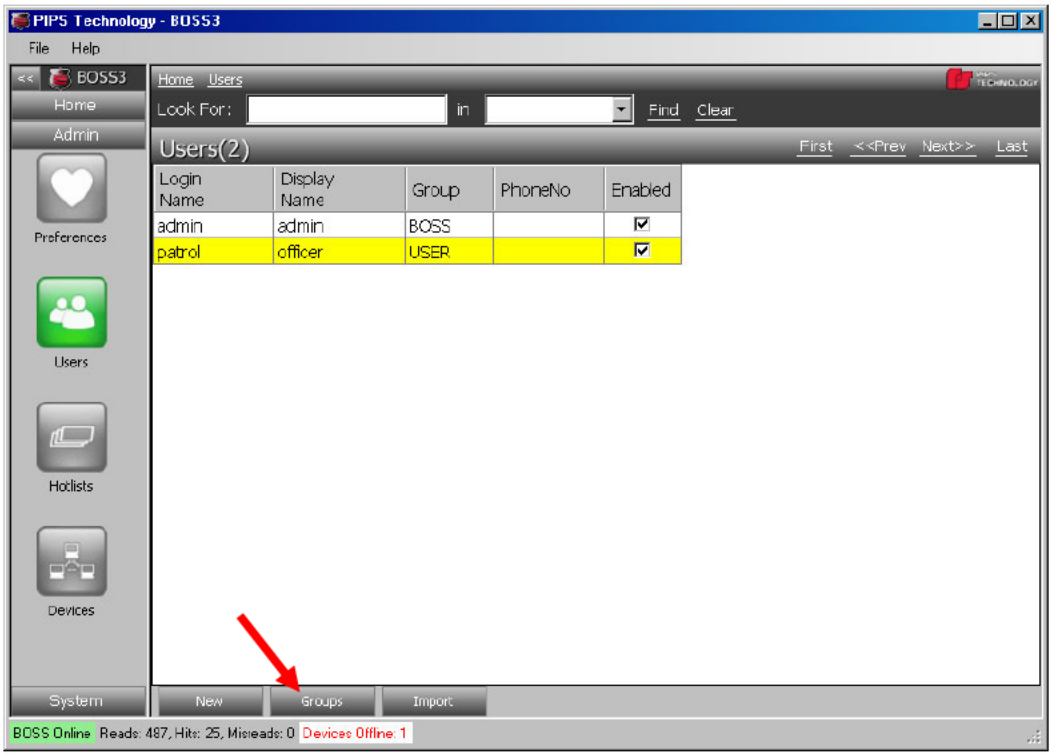


6. Hit "Save":

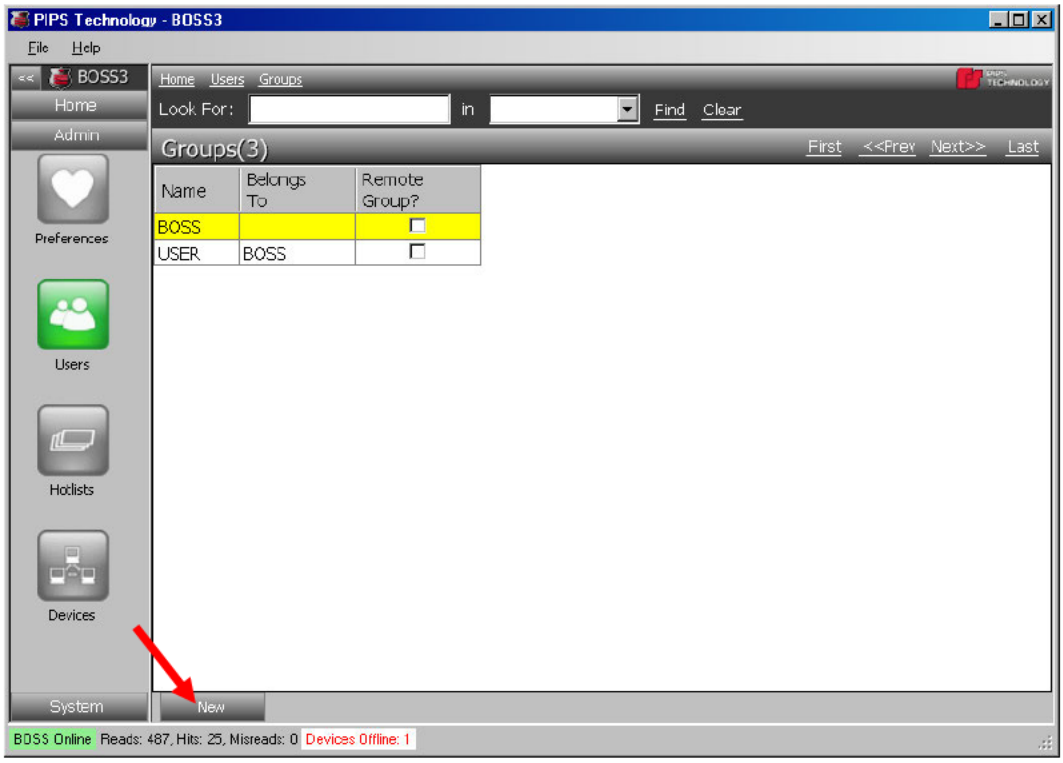


Create a new Remote Group for the other agency:

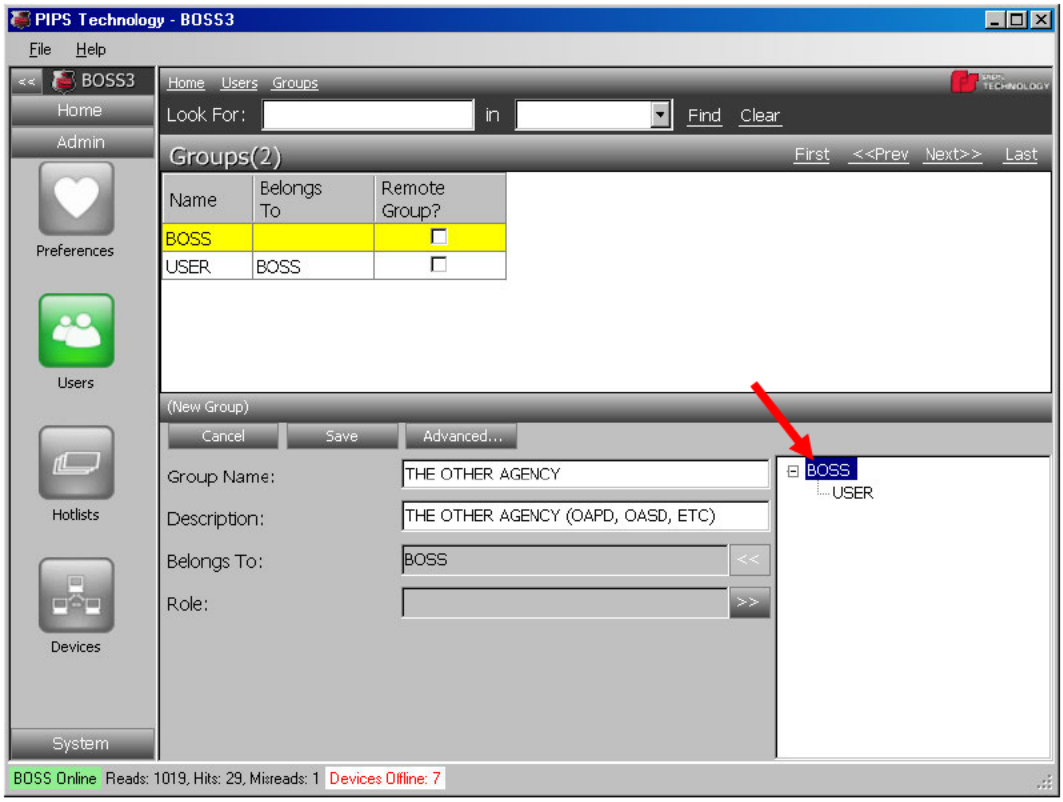
7. Click "Groups".



8. Click "New" to create the new Remote Group:

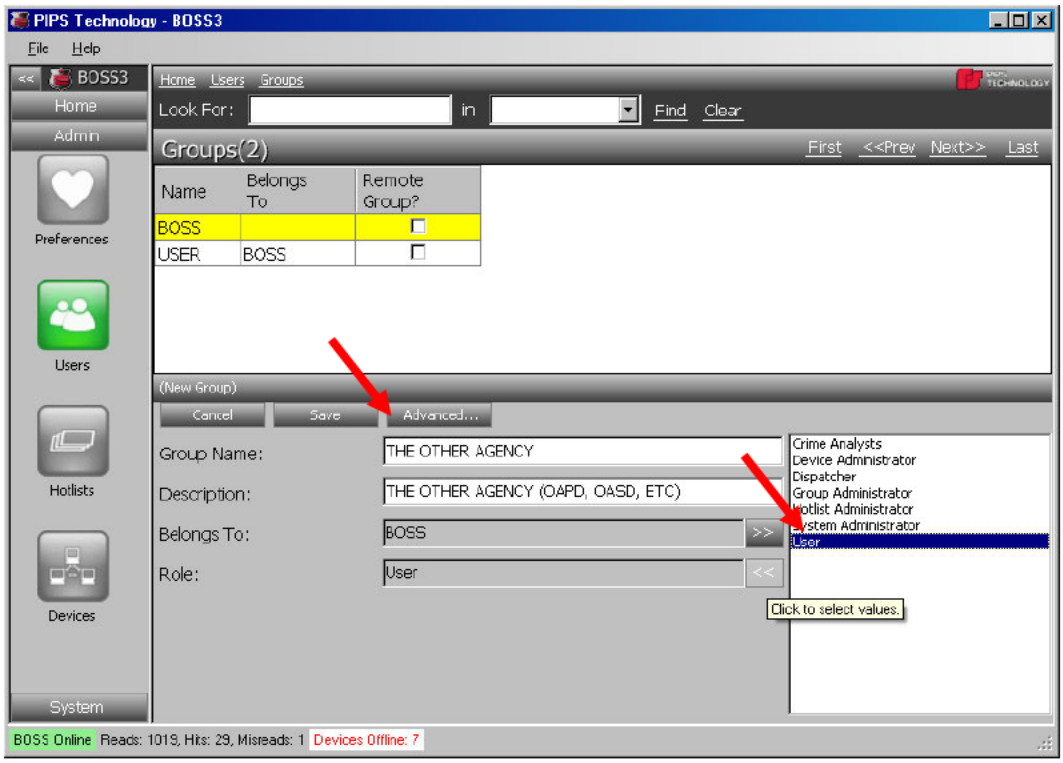


9. Name the other remote agency's group. The "Description" field is how the name will appear to BOSS users. NOTE: Group must be at top level (in most cases, click "Belongs To" and choose **BOSS** Group as shown below):

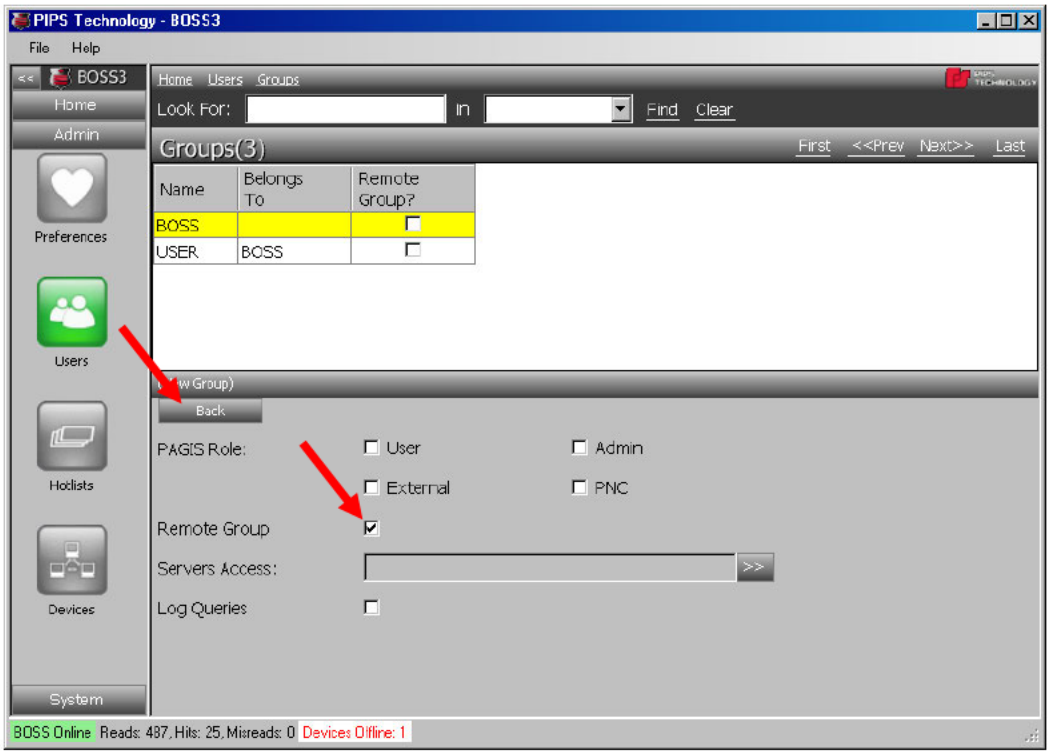


ADD a "Role" to the new "Group"

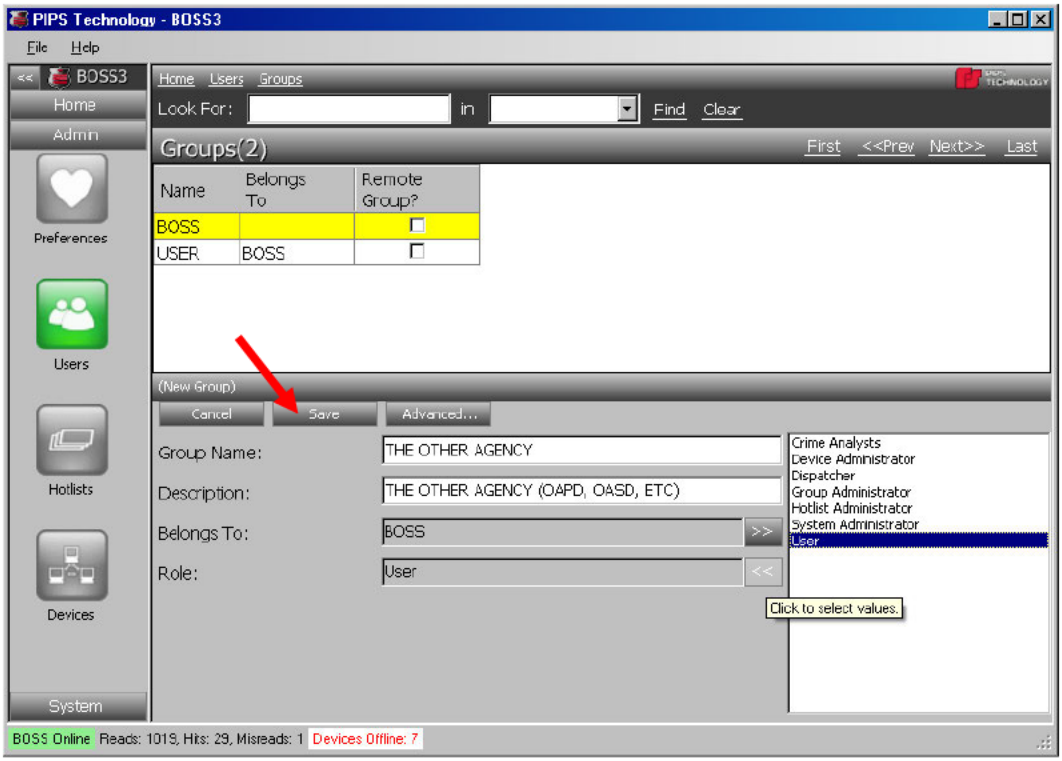
10. Add a "Role" to the other agency's group. In most cases, the "User" role is sufficient (as shown below), then click "Advanced":



11. Check the “Remote Group” box. Click “Back”:

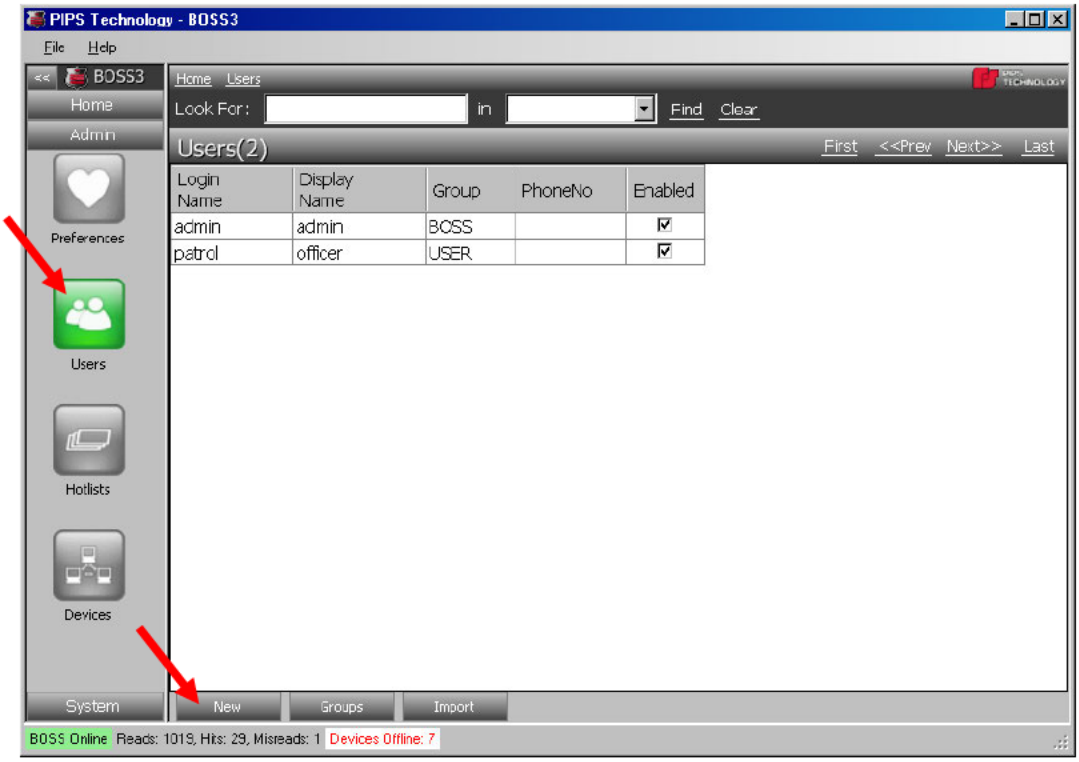


12. Click “Save”.

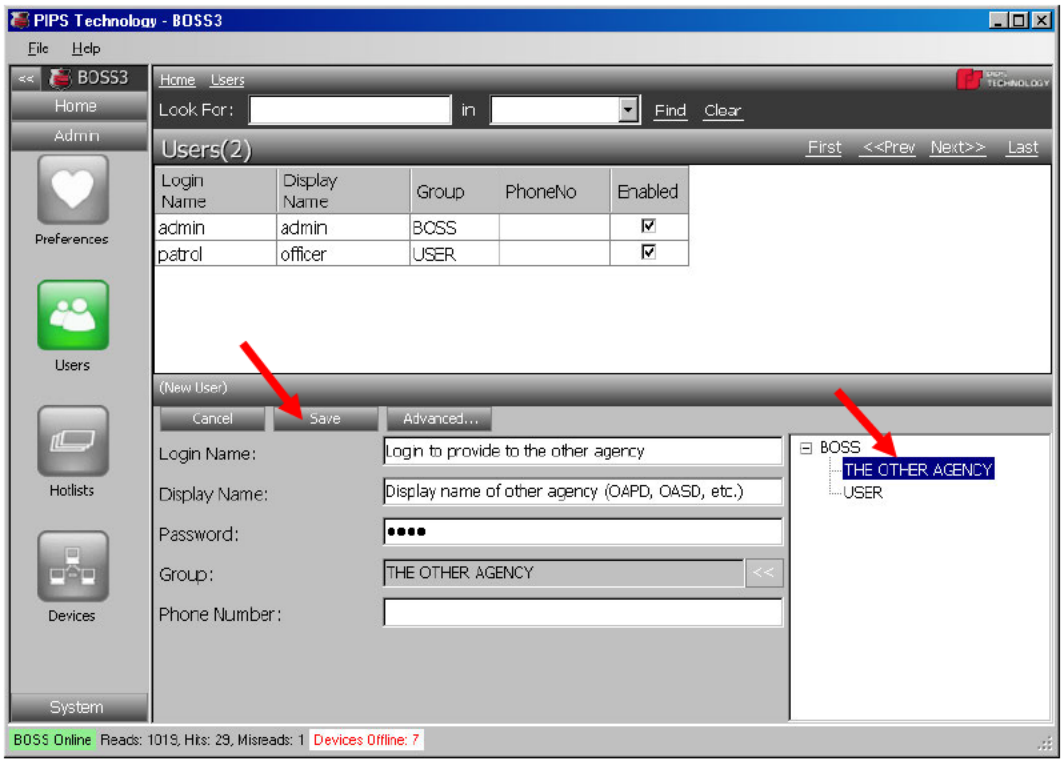


Create a User account for the other agency’s “Remote Group”

13. Click “Users”, then “New”:

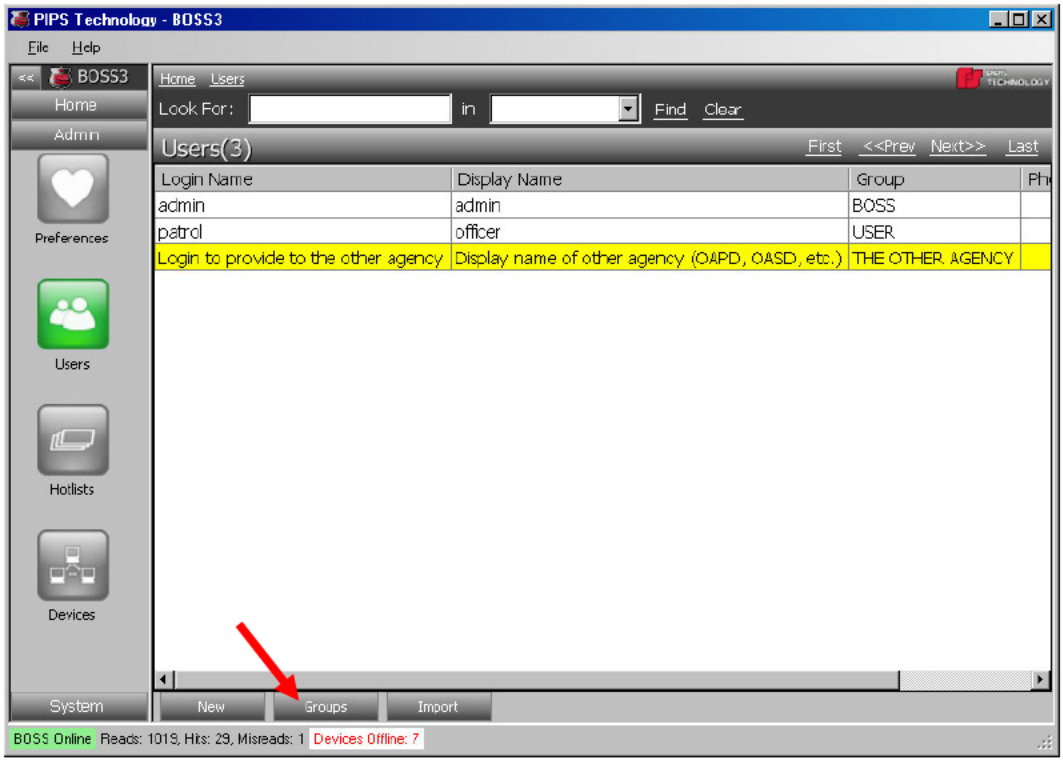


14. Assign a user login/password to provide to the other agency. Add them to the newly created remote **Group**, then click “Save”. **This is the login/password you will provide to the other agency for them to access your BOSS data.**

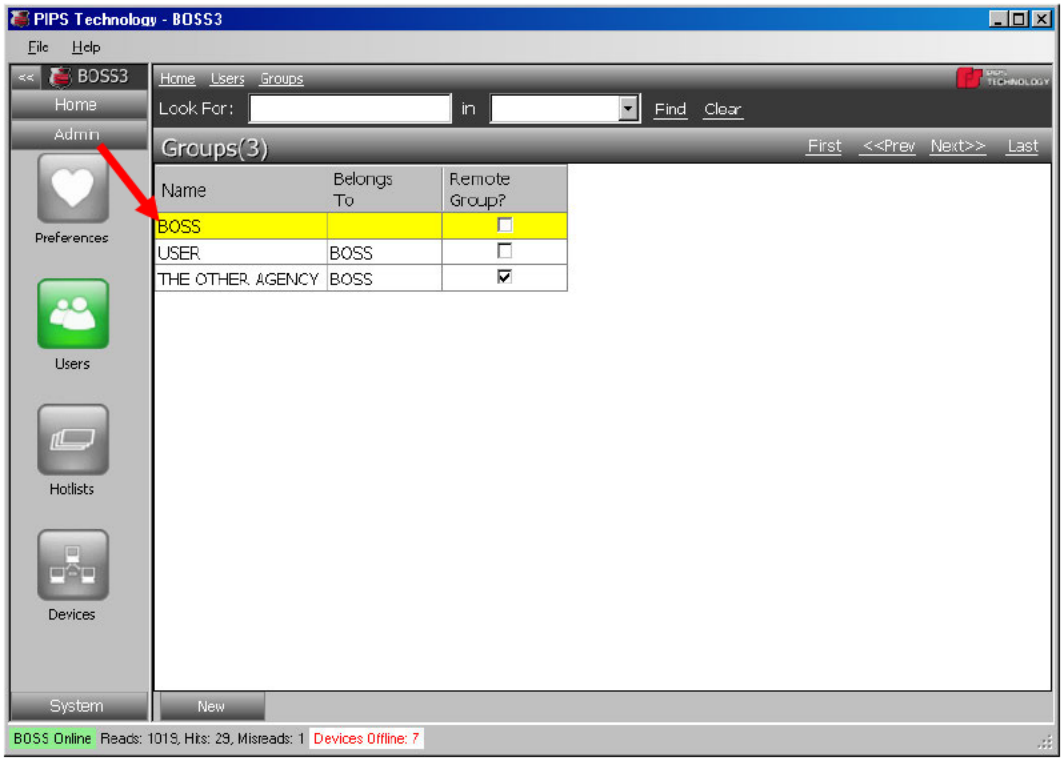


Set Group Permissions

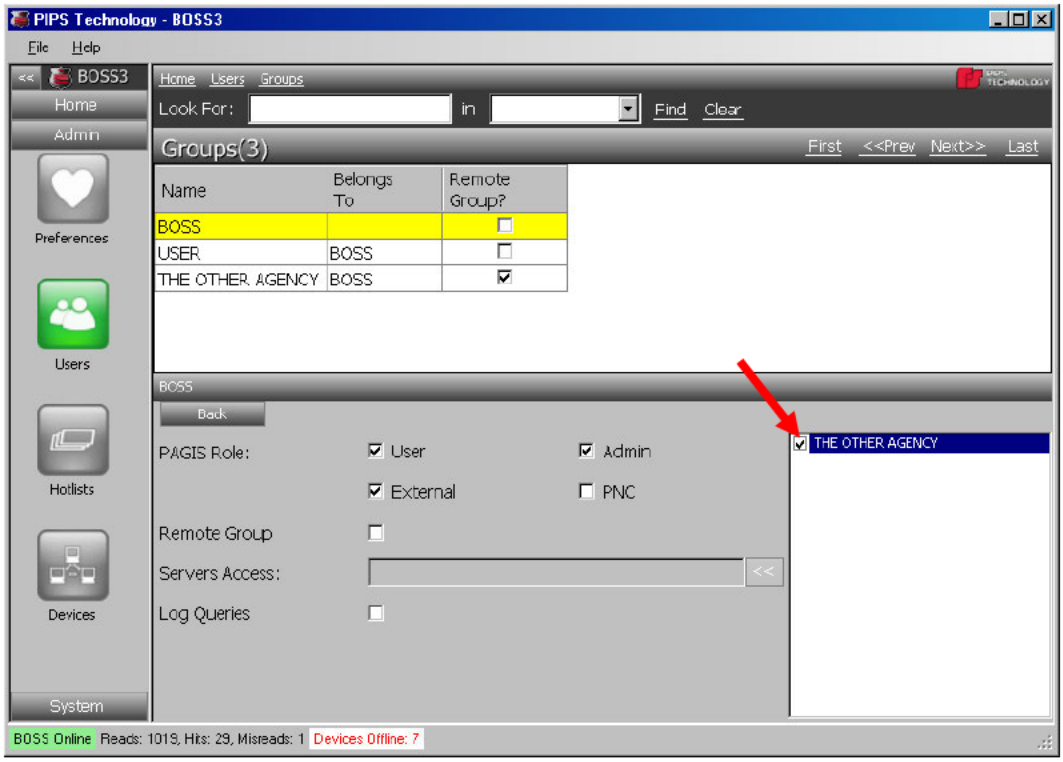
15. Give permission to YOUR AGENCY’S internal Groups to access the other Agency’s BOSS data. Click “Groups”:



16. Double click on one of YOUR agency's group to grant access to see the OTHER agency's BOSS data:

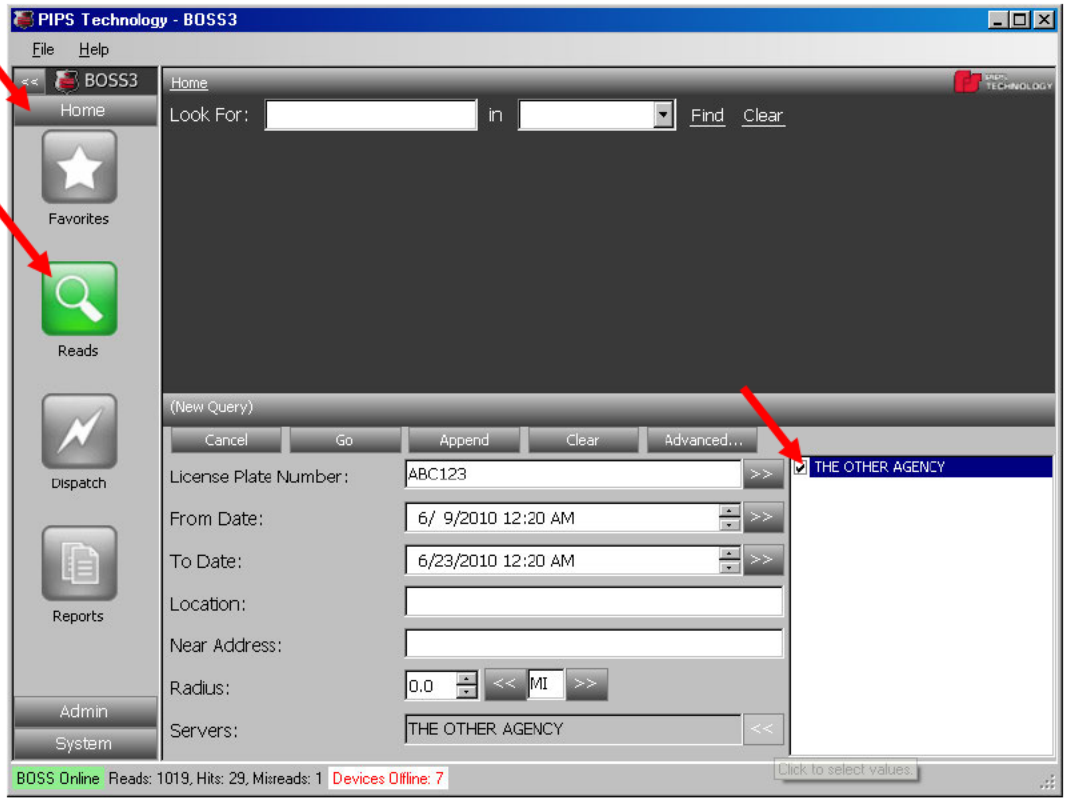


17. Click the "Advanced" button. Under "Servers Access", check the box of other agency's BOSS server. Do this for EACH GROUP that needs access to the other agency's BOSS server:



Configuration Complete-Test the connection

18. **Test the connection:** Logout, log back in. Click "Home", then "Reads" and search for a plate. Under" Servers", select the other agency's BOSS server to include it in the search.





3M™ Back Office System Software®

User's Manual

Version 3.2 or above

Table of Contents

1 Introduction 6
1.1 The Design of 3M Back Office System Software Version 3.2 and Above 6
1.2 Organization of This User's Manual 7

2 Logging In 8
2.1 3M Back Office System Software Administrator Login 8
2.2 User Login 8
2.3 Login Dialog 8
2.3.1 Storing Username and Password 9
2.3.2 BOSS Client Connection Settings 9

3 Application Layout 10
3.1 Components of the BOSS Application Screen 10
3.2 The BOSS Home Screen 11
3.3 Help Documentation 12
3.4 Minimizing the BOSS Application 12

4 BOSS Access Permissions: Users/Groups/Roles 13
4.1 Permission Levels 13
4.2 Permissions 13
4.3 Roles 14
4.4 Groups 15
4.4.1 Creating a New Group 15
4.4.2 Parent Groups 16
4.4.3 Deleting a Group 16
4.5 Users 17
4.5.1 Creating a New User 17
4.5.2 Deleting a User 18
4.5.3 Importing Users from Active Directory 19
4.6 Access Permission Example 20

5 Devices and Sites 21
5.1 Devices 21
5.1.1 Default Devices 21
5.1.2 Defining a Device 22
5.1.3 Editing a Device 23
5.1.4 Enabling and Disabling a Device 23
5.1.5 Deleting a Device 24
5.2 Sites 24
5.2.1 Default Sites 24
5.2.2 Creating a Site 25
5.2.3 Deleting a Site 25
5.3 Preferences 26
5.3.1 Changing User Preferences 26

6 BOSS Data Sharing 27
6.1 Configuring BOSS to Allow Remote BOSS Queries 27
6.2 Configuring BOSS to Access a Remote BOSS Server 27

7 Hotlists 28
7.1 Creating a New Hotlist 28
7.1.1 Configuring Basic Hotlist Settings 28
7.1.2 Defining the Hotlist Data Source 30
7.1.3 ZIP Compressed Hotlist Files 32
7.1.4 Defining Hotlist Source Credentials 32
7.1.5 Defining Hotlist Advanced Options 33
7.2 Enabling and Disabling a Hotlist 35
7.3 Modifying Hotlist Entries 35
7.3.1 Querying Hotlist Entries 36
7.3.2 Editing a Hotlist Entry 37
7.3.3 Adding a Hotlist Entry Manually 37
7.3.4 Deleting a Hotlist Entry 38
7.4 Targets 38
7.4.1 Creating a New Target 39
7.4.2 Deleting a Target 39

8 Hotlist Formatters 40
8.1 Creating a New Formatter for Hotlists 40

9 Alerts 41

10 Dispatch 42
10.1 Dispatch Settings 42
10.2 Dispatch Hits 43
10.3 Dispatch Reads 44
10.4 Manual Entries 44
10.4.1 Adding a Manual Read 44
10.4.2 Correcting Reads 45

11 Querying Stored Data 46
11.1 Wildcards 46
11.2 Quick Search Bar 46
11.2.1 Quick Search Fields 46
11.3 Query Result Navigation Icons 47
11.4 Advanced Reads Queries 47
11.4.1 Performing an Advanced Reads Query 47
11.4.2 Entering Advanced Reads Query Criteria 48
11.4.3 Managing Query Results 49
11.5 Multiple Query Tabs 50
11.6 Cross-Referencing External Data 50
11.7 Working with Queried Reads 51
11.7.1 Viewing Query Results 51
11.7.2 Query Results Actions 52
11.7.3 Viewing Read Details 52
11.8 Favorites 55
1.8.1 Creating a New Favorite 55
11.8.2 Activating a Favorite 55
11.8.3 Deleting a Favorite 56

12 Reports **57**
12.1 Running a System Report 57
12.2 Viewing and Printing Reports 57
12.2.1 Viewing the Login Statistics Report 58

13 Client Tools **59**

14 Archiving Data **60**

15 System Settings **61**
15.1 Sessions 61
15.1.1 Viewing and Disconnecting Sessions 61
15.1.2 Workstation Power Management and Sessions 62
15.2 Dispositions 62
15.2.1 Defining a New Disposition 62
15.2.2 Deleting a Disposition 62
15.3 System Parameters 63
15.3.1 Editing System Parameters 63
15.3.2 List of BOSS System Parameters 63
15.3.3 Branding 66
15.4 Roles 67
15.4.1 Adding New Roles 67
15.4.2 Deleting Roles 67
15.5 Report Management 68
15.5.1 Assigning Permissions to Access Reports 68
15.6 Translations 68
15.6.1 Entering a New Translation 69
15.7 Justifications 70
15.7.1 Entering a New Justification 70
15.7.2 Deleting Justifications 70

16 Appendix: System Requirements **71**
16.1 Minimum System Requirements 71
16.1.1 Smart Client Minimum System Requirements 71
16.1.2 BOSS Server Minimum System Requirements 71
16.1.3 SQL Server Minimum System Requirements 72
16.1.4 Client Tool Minimum System Requirements 72
16.2 Recommended System Requirements 72
16.2.1 Smart Client Recommended System Requirements 72
16.2.2 BOSS Server Recommended System Requirements 72
16.2.3 SQL Server Recommended System Requirements 73
16.2.4 Client Tool Recommended System Requirements 73

17 Appendix: Installation and Configuration Guide **74**
17.1 Installing the BOSS Server Application Files 74
17.1.1 Running the Installer 74
17.1.2 3M License Agreement 75
17.1.3 Selecting the Installed Components 76
17.1.4 Selecting the Installation Folder 77
17.2 BOSS Version 3.2 and Above License Key Management 79
17.2.1 Activating the License Key 79
17.2.1.1 Activating the License Key over the Internet 80
17.2.1.2 Activating the Software with a License File 81
17.2.1.3 Request a License File to Activate the License 81
17.2.2 Updating a License Key 82
17.3 Map Display Options with BOSS 83
17.3.1 U.S. Census Bureau TIGER Maps 83
17.3.2 Advanced Mapping with Microsoft Bing Maps 83
17.4 Configuring the BOSS Server Application 83
17.4.1 The BOSS Controller Application 83
17.4.1.1 Starting the BOSS Controller 83
17.4.1.2 Status Colors 84
17.4.1.3 Right-Click Menu 84
17.4.1.4 Starting the BOSS Service 84
17.4.1.5 Stopping the BOSS Service 84
17.4.2 BOSS Configuration 85
17.4.2.1 Activating the Configuration Wizard 85
17.4.2.2 BOSS Configuration Wizard 85
17.4.2.3 SQL Server Configuration 86
17.4.2.4 Resetting the Administrator Password 87
17.4.2.5 Network Port Settings 87
17.4.2.6 Regional Hotlist Formatters 89
17.4.2.7 NCIC Hotlist Formatters 90
17.4.2.8 TIGER Maps Configuration 90
17.4.2.9 Finishing Configuration 93
17.5 Installing the BOSS Smart Client Application 94
17.5.1 Installation over the Web 94
17.5.2 Stand-Alone Installation 94
17.6 Configuring Client Tools 94
17.7 The BOSS Upgrade Tool 95

18 Troubleshooting **96**

19 Appendix: Plug-Ins **100**
19.1 The BOSS Truck Drayage Utility 100
19.2 The BOSS LPRD Plug-In 100
19.3 The BOSS DEA Plug-In 100

20 Appendix: GNU Lesser General Public License **101**

Glossary **107**

Index **108**

Notices

The information within this manual is authorized for distribution to customers, authorized service center personnel, and distributors of 3M. Every effort has been made to supply correct information. However, 3M 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. 3M 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 your system.

Warranty

Warranty and Limited Remedy: 3M warrants that the 3M product will be free from substantial defects in material and workmanship under normal use and service, wear and tear excepted, for twelve (12) months from the date of shipment. For software products, for twelve (12) months from the date of shipment, the software will materially perform the functions described in the accompanying documentation. 3M MAKES NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS, INCLUDING ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. If the 3M product does not conform to this warranty, the sole and exclusive remedy is, at 3M's option, repair or replacement of the 3M product or refund of the purchase price.

Limitation of Liability: Except where prohibited by law, 3M will not be liable for any loss or damage arising from the 3M product, whether direct, indirect, special, incidental or consequential, regardless of the legal theory asserted.

Technical Support

Service of this equipment by replacement of parts, on-site repair, or routine maintenance inspections is available. Please contact 3M Motor Vehicle Services and Systems.

Phone: 877-777-3571
Email: ALPRSupportUS@mmm.com

Web: www.3M.com/mvss

Fax: 800-591-9293

3M Center
Building 235-3A-09
St. Paul, MN 55144

Design Changes

3M 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

The 3M camera series, 3M™ License Plate Capture Software®, 3M™ Back Office System Software®, are registered trademarks of 3M. Windows®, Windows Vista®, Windows 7, Windows 8, Bing®, and Microsoft® .NET are all trademarks of the Microsoft Corporation. Other trademarks and registered trademarks are the property of their respective owners.

Copyright

3M Back Office System Software is copyright © 2006-2014 3M Company. All rights reserved. This product contains confidential and trade secret information of 3M, 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.

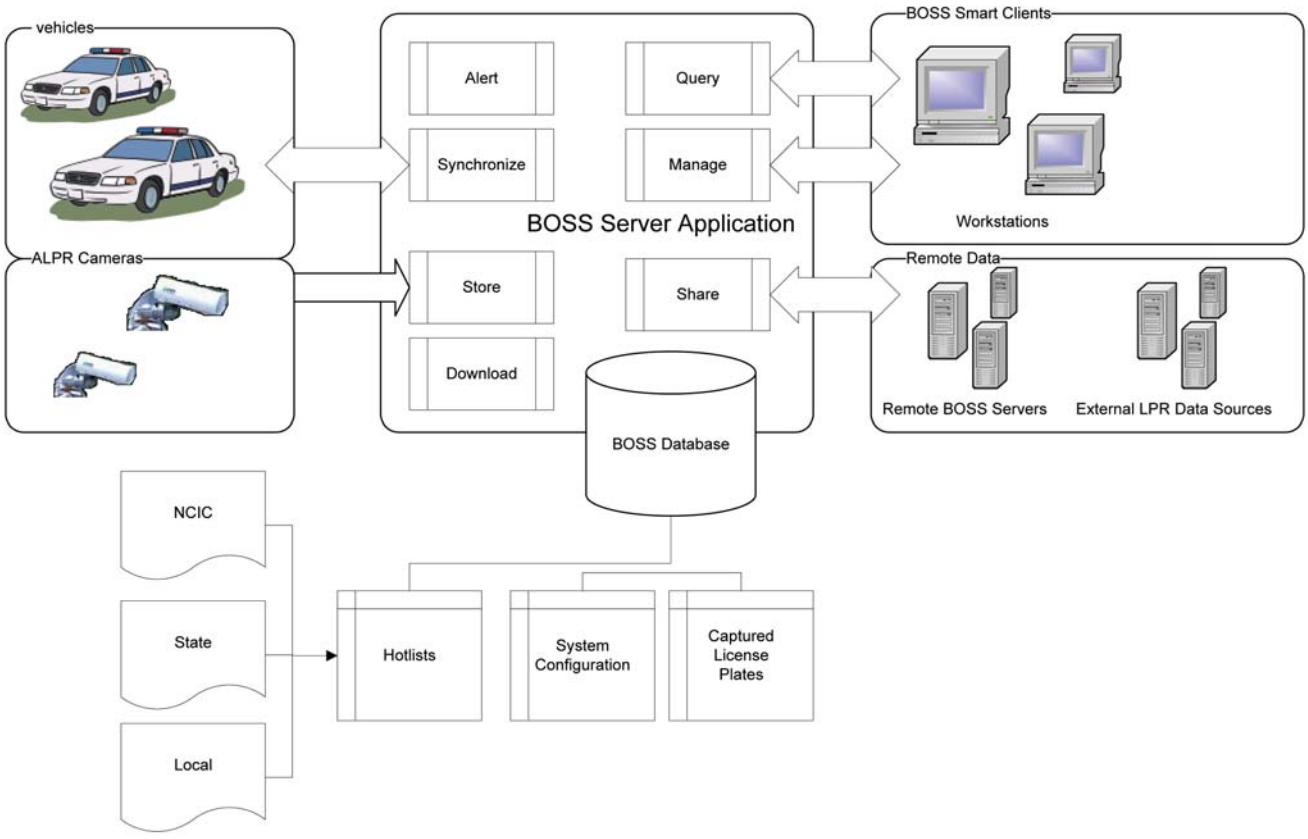
Version

The manual documents the 3.2 series version of the BOSS software. The document was last updated on March 27, 2014.

1 Introduction

This document serves as a user's manual for the 3M Back Office System Software (BOSS) version 3.2 or above and describes the various features and functionality of the application. BOSS is a management and administration tool for the 3M Automatic License Plate Recognition (ALPR; also known as ANPR, or Automatic License Number Recognition) systems. The BOSS server application provides an interface for user maintenance, data queries, import and export of data, and dispatch functions. BOSS lets an Administrator specify the databases used by both mobile and fixed camera installations. BOSS retrieves these databases on a regular schedule; manages the users of the 3M™ License Plate Capture Software (LPCS) systems and BOSS Smart Client workstations; provides a central repository for data collected by mobile LPCS deployments and fixed camera installation; provides reporting and data management tools; provides hit detection and dispatch functions for fixed camera installations; and allows for data mining and data sharing with other agencies.

The following schematic shows how the BOSS server application works together with Smart Client workstations, various data sources, LPCS, and the full line of ALPR cameras to create a comprehensive solution.



1.1 The Design of 3M Back Office System Software Version 3.2 and Above

The design of BOSS version 3.2 or above offers ease of accessibility with a user-friendly look and feel. Large, easy-to-identify icons provide intuitive navigation, and the frequently used elements are readily available. The user interface (UI) is very recognizable and comfortable, particularly for users already familiar with Windows-based applications, including Microsoft® Office software, or the 3M License Plate Capture Software. In addition, users can enter a minimum amount of information to add a data object, with the ability to include more details if needed.

1.2 Organization of This User's Manual

The *3M Back Office System Software, Version 3.2 or above, Software User's Manual* guides BOSS users and Administrators through the following topics:

- Logging in
- Application Layout
- Access Permissions: Users/Groups/Roles
- Devices and Sites
- Data Sharing
- Hotlists
- Hotlist Formatters
- Alerts
- Dispatch
- Querying Stored Data
- Reports
- Client Tools
- Archiving Data
- System Settings

The appendices provide system requirements for BOSS servers and Smart Client workstations and a guide to installation and configuration. Additional appendices cover troubleshooting and BOSS plug-ins. A glossary of commonly used terms and acronyms follows the appendices.

2 Logging In

2.1. 3M Back Office System Software Administrator Login

During each new installation of the 3M Back Office System Software, a default user of “admin” is created, with the password of “admin1.” The installer or designated BOSS Administrator can log in with this account to create additional users and otherwise configure the system. It is important that the “admin” password be changed in order to protect the system’s security. Likewise, it is equally as important to keep this and all passwords confidential in order to protect the security of the BOSS system. Section 17, Installation and Configuration, offers more information on setting up users and passwords.

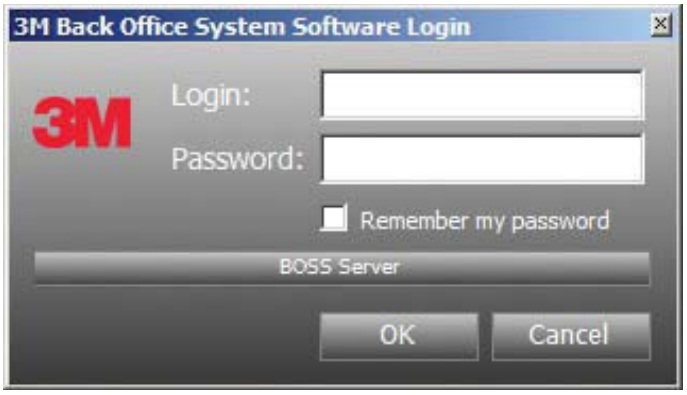
2.2 User Logins

The 3M Back Office System Software will require a user to log in with a username and password only if there is no BOSS user matching the current Active Directory user login. In other words, if the username currently logged into Windows matches a username in the BOSS system, the user is automatically logged into the application when it is started, and no login screen will appear.

For example, if user “bsmith” is logged in using Windows Domain Authentication through Active Directory (“logged into Windows”), when the BOSS Smart Client is started, and a “bsmith” user exists within the BOSS system, no login screen will appear; the application will authenticate the user and load automatically. If a user logs onto Windows with a name that is not an exact match to a username in the BOSS system, or is not logged into the same Windows Domain, a login screen will appear. The user will then need to enter a correct BOSS user name and password in order to enter the application.

Note: In order for a user to be automatically logged into BOSS, the Active Directory user must be in the same Windows domain as the 3M Back Office System Software server.

2.3 Login Dialog



1. Enter your username in the Login field.
2. Enter the correct password in the Password field. **Note:** Passwords are case sensitive.
3. Click **OK** to complete the login process.

2.3.1 Storing Username and Password

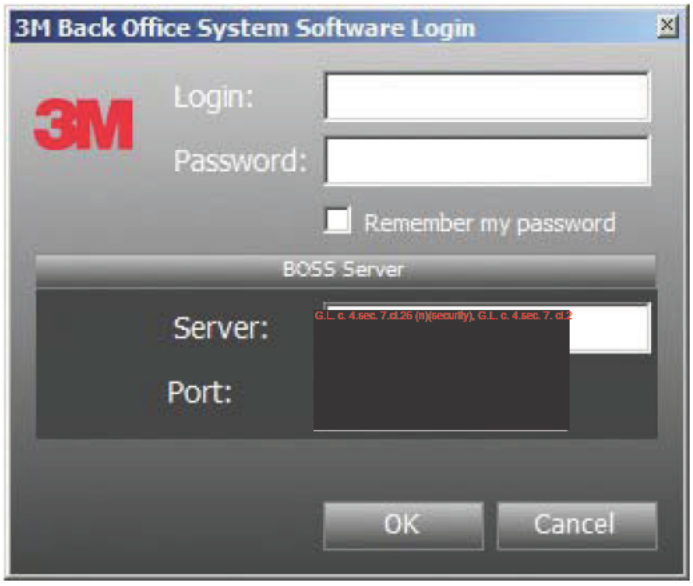
Select the **Remember my password** option to save the password to the computer's local Windows registry and automatically fill in both Login and Password fields on subsequent logins.

Selecting this option only remembers the login information for the current Windows User on the local computer. It will not apply to a different Windows user logged in the same computer and will not apply to the same user logging in a different computer. This option need not be checked every time. Once checked, the option will stay that way until it is deselected during a login.

Note: The username and the password are stored in the Windows Registry. This can be a security risk. It is recommended that you not use the **Remember my password** option unless the Windows workstation can be secured against unauthorized access.

2.3.2 BOSS Client Connection Settings

Click the **BOSS Server** button on the Login screen to view or change the client connection settings.

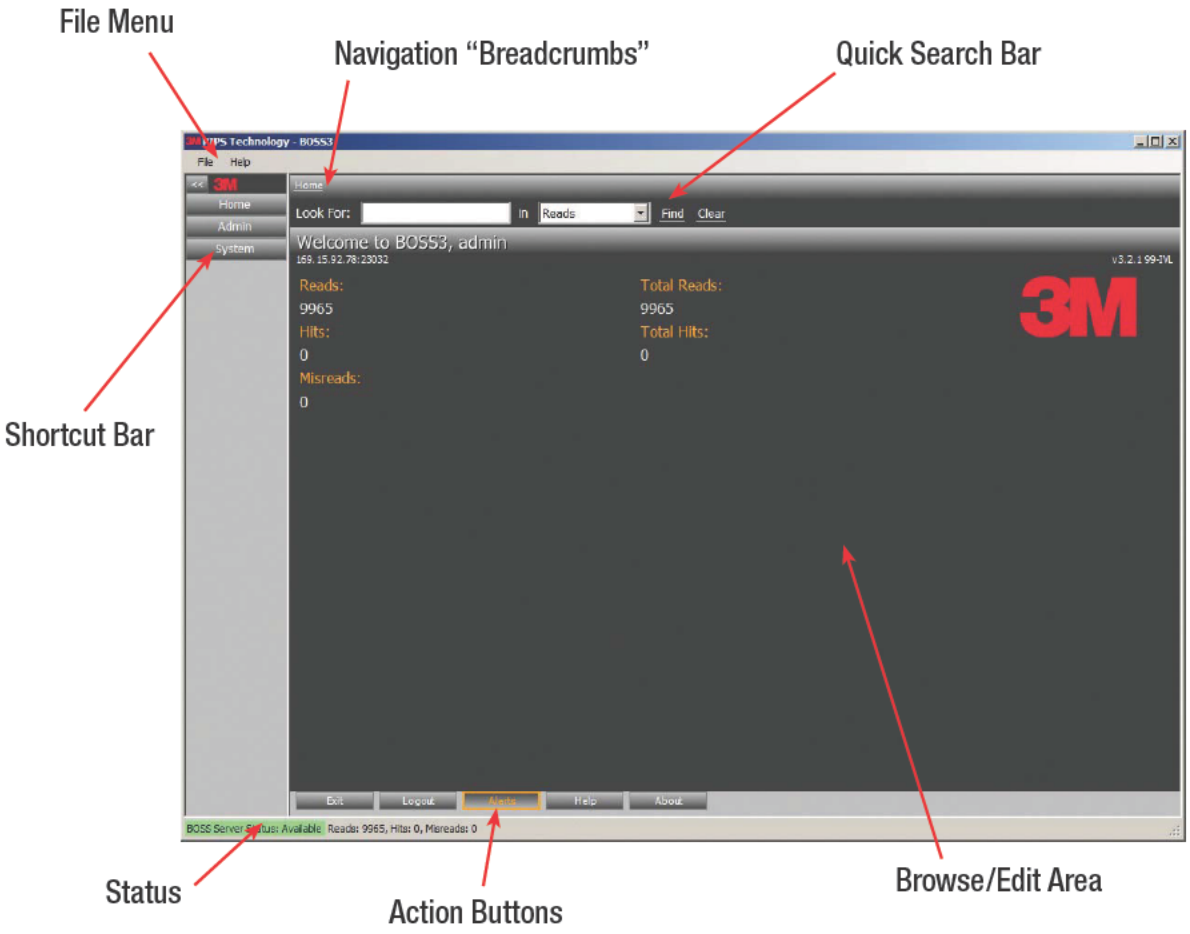


Server – IP address, computer name, or DNS address can be used in the Server field as long as the client can reach the server using the value entered.

Port – The default port used for connecting to the BOSS server is 23032. This should only be changed here if the BOSS server has been configured to use a non-default port.

3 Application Layout

3.1 Components of the BOSS Application Screen



File Menu – The File menu of the application resides in the very top left of the application window. The File menu is always visible and available regardless of the screen or shortcut selected. The **Exit** option is available through this menu.

Navigation – The navigation "breadcrumbs" appear at the top of the BOSS screen as different actions are selected. By clicking on the links it is possible to backtrack to a previous screen.

Shortcut Bar –The Shortcut bar (the panel on the left of the screen) contains icon buttons for the various operations available. The shortcut icons are divided into three categories: **Home**, **Admin**, and **System**. Each time the application is started, all of the categories are closed with no shortcuts displayed. Click on any of the three headings to access the shortcuts within that category. The actual categories and shortcuts that appear depend on the logged-in user's privileges.

The Shortcut bar can be collapsed entirely to provide a larger space for the Browse/Edit area by clicking the << button at the top left of the screen. To expand the Shortcut bar again, click the >> button.

Browse/Edit Area – The widest portion of the application window, the Browse/Edit area is where data is displayed for viewing or editing. The actual data displayed here depends upon the shortcut icon that is selected from the Shortcut bar.

Quick Search Bar – Directly above the Browse/Edit Area, the Quick Search bar allows for simple, immediate queries of BOSS data. Using the

Quick Search bar simply involves typing the text to query in the **Look For** field and selecting the type of data (reads, hits, etc.) to search in the drop-down box.

Action Buttons – These are the buttons directly below the Browse/Edit area. These buttons will differ depending on the shortcut icon selected. The actual buttons that appear will also vary depending upon the user's privileges.

Status Bar – This is the area along the very bottom of the application window that displays the following system information:

- **BOSS System State** (Available or Offline): "Available" status indicates that the client is currently communicating with the BOSS server application and the server is running. This status is highlighted with a green background. "Offline" status indicates that the client is currently not able to communicate with the BOSS server and is highlighted with a red background. In this event, the BOSS UI will continue to check for the BOSS server to become available again. After three attempts to reconnect, the user will be notified that the connection could not be re-established and will be provided further instructions on how to proceed.
- **Reads:** The total number of reads currently contained in the BOSS system.
- **Hits:** The total number of hits currently contained in the BOSS system.
- **Misreads:** The total number of misreads currently contained in the BOSS system.
- **Devices Offline:** The number of fixed camera devices that are currently identified as offline.

3.2 The BOSS Home Screen

The BOSS Home screen is displayed within the Browse/Edit area upon login. The top banner displays the username of the current BOSS user, the BOSS server address, and current system statistics. Statistics may take a few moments to update after login. The action buttons, described below, are displayed along the bottom of the screen. The actual buttons that display will vary depending upon the user's privileges.

Exit – Exit the BOSS application.

Logout – Log out from the current session to the Login screen.

Alerts – Toggle dispatch alerts on (orange highlight) and off. This button will not be displayed if the user is not authorized to access the dispatch screen, or if the user has not chosen to receive dispatch alerts in Preferences *(Section 5.3)*.

Help – Activate the help system.

About – Display application information.

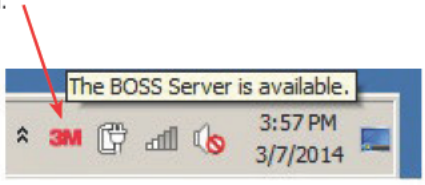
3.3 Help Documentation

BOSS provides a help document accessible in the client application. To access help, select **Help** in the File menu area or press the **F1** button. A help document will be displayed in a browser window and is indexed and searchable for ease of use.



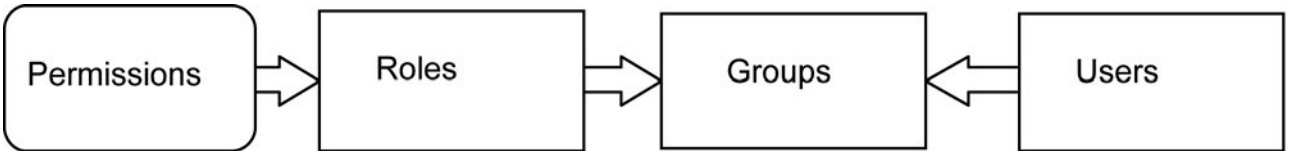
3.4 Minimizing the BOSS Application

The BOSS application can be minimized to the Windows System Tray using the Windows minimize button on the right upper corner of the BOSS application window. To restore the BOSS application, click on the **BOSS 3M** icon. When the application is minimized, real-time alerts will still be displayed.



4 BOSS Access Permissions: Users/Groups/Roles

Access permissions to various functions (such as reports or dispatches) in BOSS are administered through users, groups, and roles. Each individual who will use the BOSS software must log in via a user account. Each user account is assigned to a group. Every group is assigned a role (such as Administrator or Dispatcher), which determines the set of functionality to which the group's members will have access:



The security parameters defined in a role apply to a user via the group to which the user belongs.

4.1 Permission Levels

The following table lists the levels that apply to permissions:

LEVEL	EXPLANATION
No Access*	No permissions to the function
Read Only	View-only permissions to the function. Add/Change/Delete are not permitted.
Full Access	Complete permissions to the function. View/Add/Change/Delete are permitted.

**When a user's effective permissions to a function are No Access, the function is not visible to the user. For example, if a user has No Access privileges to the System function, the System category is not displayed.*

4.2 Permissions

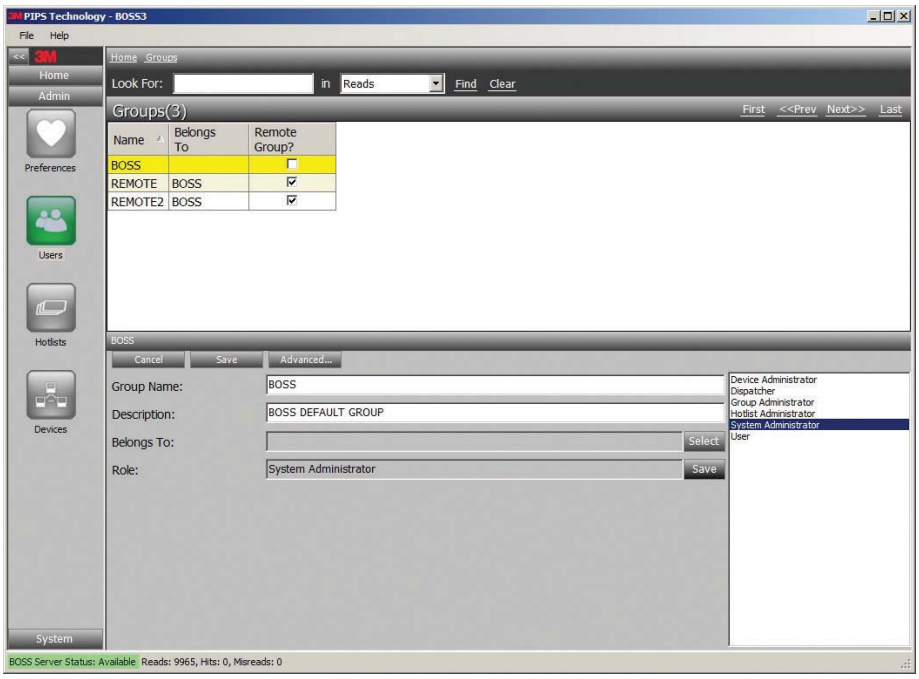
The following table lists the functions that are controlled by permissions levels:

PERMISSION	EXPLANATION
Reads	Plate read information
Dispatch	Real-time monitoring and hit alerts
Users	Groups and user accounts
Hotlists	Hotlists (plates of interest)
Devices	Sites and ALPR camera devices
System	System configuration options

See Section 15.4, Roles, for more information on setting permissions.

4.3 Roles

Roles are access permission profiles. BOSS comes with several predefined roles. A BOSS Administrator is able to add additional roles to the system. A BOSS Administrator is also able to alter and delete any roles. Roles define a **permission level for different functions** of the system. *See Section 15.4, Roles, for additional information.*

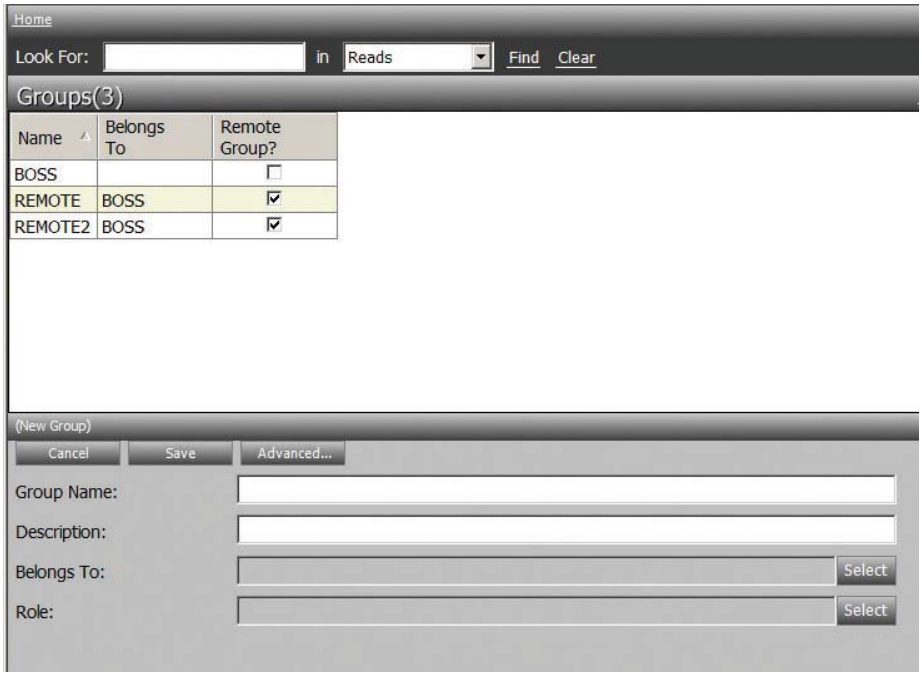


The following roles are installed by default in a BOSS system:

- System Administrator
- User
- Dispatcher
- Group Administrator
- Device Administrator
- Hotlist Administrator

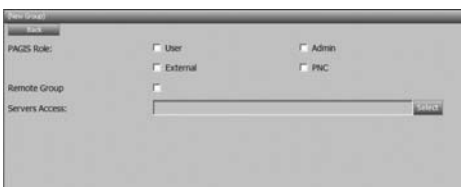
4.4 Groups

Groups are collections of users that have the same permissions. Groups provide an efficient way to organize users, for example by organizational units, and easily assign permissions to those users. Using groups is optional. A default group named “BOSS” automatically exists within a BOSS system, and user accounts will belong to the “BOSS” group by default. The BOSS group cannot be deleted.



4.4.1 Creating a New Group

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut. A list of all current users will display in the Browse/Edit area.
3. Click the **Groups** button at the bottom of the Browse/Edit area. A list of all current groups will display in the Browse/Edit area.
4. Click the **New** button. The New Group Entry screen will display.
5. In the Group Name text box enter a name for the group. (**Note:** The group name must have a minimum of three characters.)
6. In the Group **Description** text box enter a description of the group (optional).
7. Each group, except for the default BOSS group, is required to have a parent group. In the Belongs To field, click the **Select** button to view a list of all existing groups. Click on the desired group and click the **Save** button to select. The name of the selected group will display in the Belongs To field as the parent group.
8. Assign a role to the group. In the Role field, click the **Select** button to select from the existing roles. Click the desired role from the list and click the **Save** button to make the selection. The name of the selected role will appear in the field.
9. Click the **Advanced…** button to access additional, optional settings for the new group.



4.4.1 Creating a New Group *(continued)*

PAGIS Role (User/Admin/External/PNC) – Check desired PAGIS (now LPCS) roles to grant the new group for the associated permissions in LPCS. *Please refer to the 3M License Plate Capture Software User's Manual for more information.*

Remote Group – Select this option to designate the group as remote. When a BOSS Administrator wants to give access to another BOSS system for remote queries ("data sharing," *see Section 6*), a login must be created and assigned to a group that is flagged as a remote group. The remote BOSS Administrator will then create a remote site with credentials for that login.

Servers Access – This option allows for defining which, if any, sites will be accessible by this group. Click the **Select** button to access a list of sites.

Note: There are two sites defined by default: Manual Entries and Unassigned. If no additional sites have been defined, only the default values are available in this field. Click each desired site and click the **Save** button to complete the selection process. If one site is selected the name of that system will appear in the Server Access field. More than one site can be selected.

Log Queries – This option, when selected, will result in the logging of all queries made by all users of the group. This information is then available via the audits report. **WARNING:** ***This can potentially be a very large amount of data. Select this option with care.***

a. Configure these Advanced User settings as desired.

b. Click the **Back** button to return to the main New Group Entry screen

10. Click **Save** to complete creating the new group, or click **Cancel** to clear the new group.

4.4.2 Parent Groups

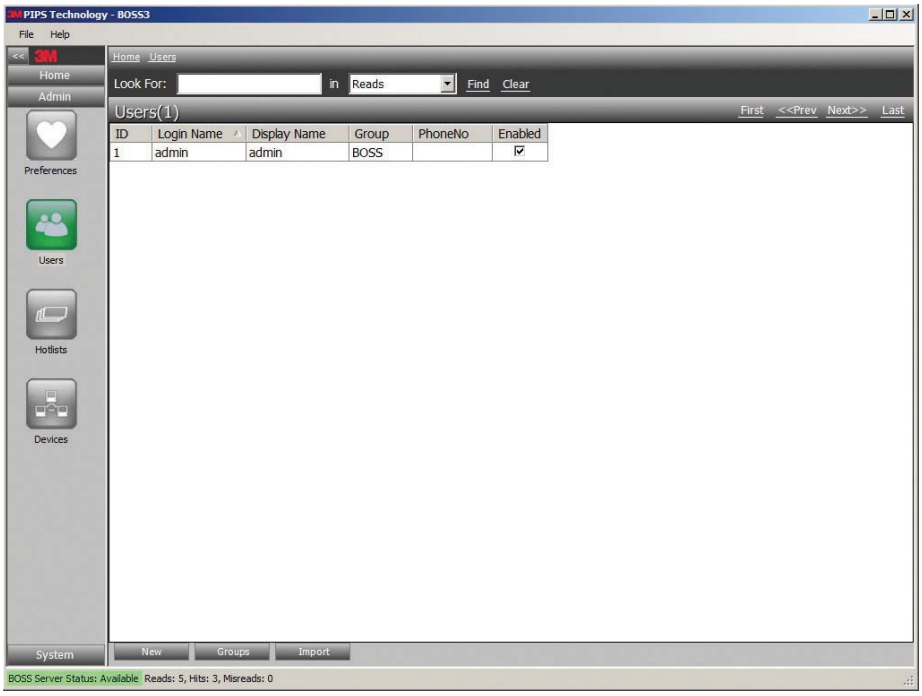
When creating a new group, you must select a parent group (the Belongs To field). BOSS uses a parent-child group structure as an organizational mechanism. This allows the BOSS Administrator to arrange groups into collections based on location, job role, or any other applicable criteria. In BOSS, the parent group can be selected in order to easily reach the entire collection of groups under that parent. This can be especially helpful in large installations with a large number of groups.

4.4.3 Deleting a Group

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut.
3. Click the **Groups** button at the bottom of the Browse/Edit area. A list of all existing groups will display in the Browse/Edit area.
4. Click to select the desired group from the list.
5. Click the **Delete** button.
6. Click **OK** in the confirmation dialog to complete the operation.

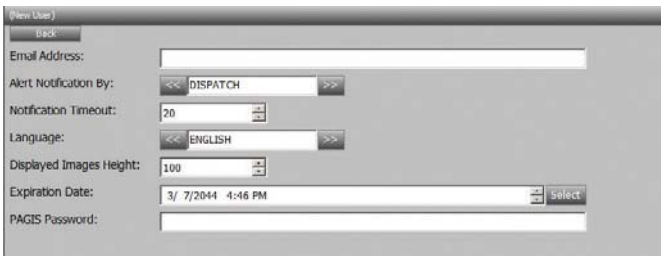
WARNING: Any users currently assigned to the deleted group will be assigned to the default "BOSS" group. You should empty the group by assigning all of its users to different groups prior to deleting it.

4.5 Users



4.5.1 Creating a New User

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut. A list of all existing users will display in the Browse/Edit area.
3. Click the **New** button at the bottom of the Browse/Edit area. The New User Entry screen appears.
4. Enter a **Login Name** for the new user. This is the name the user will enter when logging into the BOSS application. (The login name must be at least three characters.)
5. Enter a **Display Name** for the new user (optional).
6. Enter a **Password** for the new user. (The password must be at least three characters.)
7. Select a **Group** for the user. Click the **Select** button to access a list of all groups. Click on the desired group and click the **Save** button to complete the selection.
8. Enter a contact **Phone Number** for the user (optional). This field is for informational purposes only; in case the BOSS Administrator needs to contact the user.
9. Click the **Advanced…** button to access additional, optional settings for the new user. Configure these advanced user settings as desired.



4.5.1 Creating a New User *(continued)*

Email Address – Email address or addresses associated with the user. BOSS alerts for the user are sent to the email addresses specified here. Multiple addresses should be separated with a comma.

Alert Notification By – A user can be configured to receive BOSS alerts through the Dispatch application, email, or both. Click the << or >> buttons to cycle through the options, stopping at the desired selection.

Notification Timeout – The cutoff time from the time when a hit occurred after which an alert will no longer be sent to the user. For example, if the notification timeout is 20 minutes and a plate of interest is detected at 12:00 pm, notification is not sent to the user after 12:20 pm. This timeout prevents alerts being sent for events that are delayed in arrival to BOSS.

Language – The language preference for the user. The default value is English.

Displayed Images Height – This setting defines the vertical size in pixels of the images (reads and hits) that will display for the user on the Dispatch and Reads screens.

Expiration Date – Date for the user account to automatically be disabled. If no expiration is desired, simply leave this field at its default value (30 years from current date).

PAGIS Password – The user's LPCS password.

Note: The user must be in a group that has been granted LPCS permissions in order for the user to log in to 3M License Plate Capture Software.

---

10. Click the **Back** button to return to the main New User Entry screen.
11. Click the **Save** button to complete creating the new user.

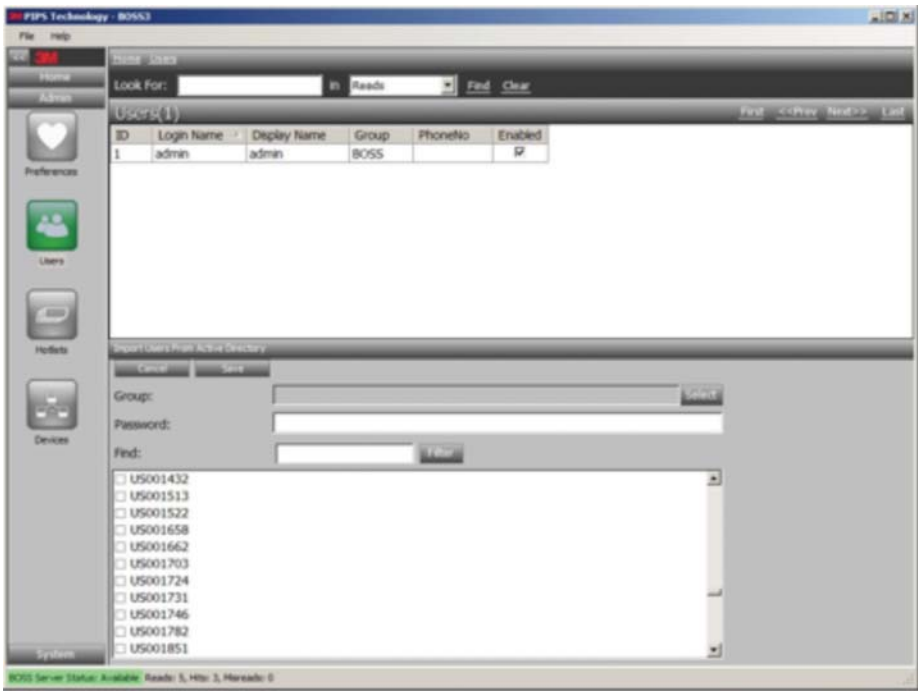
4.5.2 Deleting a User

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut. A list of all existing Users will display in the Browse/Edit area.
3. Click the desired user in the list.
4. Click the **Delete** button at the bottom of the Browse/Edit area.
5. Click **Yes** to confirm the operation.

4.5.3 Importing Users from Active Directory

BOSS allows user logins to be imported from Microsoft Active Directory (AD) service.

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut.
3. Click on the **Import** button.



4. Select the BOSS group that will receive the imported logins. Click the **Select** button to display available groups and **Save** to commit the selection.
5. Enter the default password for the imported logins in the Password field.
6. Browse for the desired users, ***or*** type in the desired login name (full or partial) in the Find field and press the **Filter** button.
7. Click on the checkbox in front of the desired usernames to select users to be imported to BOSS.
8. Click on **Save** to import the users from Active Directory.

Note: A Windows login cannot have any punctuation included or problems will occur with reads queries being performed.

4.6 Access Permissions Example

The previous sections have described how BOSS user security is designed, using roles, groups, and user accounts. This section presents a working example that integrates the information in this chapter.

A BOSS Administrator creates a role, names the role “Temporary Workers,” and defines the new role to have very limited permissions, as follows:

Reads	Read Only
Dispatch	Read Only
Users	No Access
Hotlists	No Access
Devices	No Access
System	No Access

Then the Administrator creates a group called “Temps.” When creating the group, a role is required. The Administrator selects the new role just created “Temporary Workers,” which assigns the permissions, defined above, to the new group.

Next, the Administrator creates a user account, “Jsmith,” for a temporary worker. While creating the new user, the Administrator is required to select a group for the user, and assigns the user to the “Temps” group just created.

The user “Jsmith” has now been created with the permissions shown above because he belongs to the group called “Temps” and that group was assigned the “Temporary Workers” role.

As this example shows, this security design allows reusability of security roles because a BOSS Administrator can define a set of permissions in a role, and that role can be assigned to multiple groups.

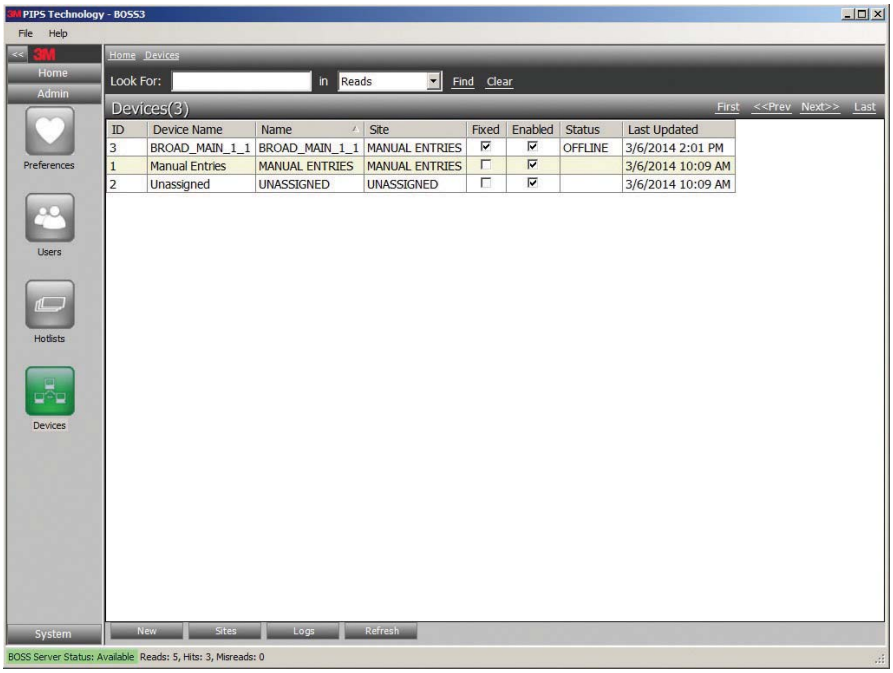
5 Devices and Sites

5.1 Devices

A BOSS device is any source that can input reads into the system. Typically, a device is a camera—either fixed or mobile (mounted on a vehicle). Another source for reads is manual entry, in which a BOSS user types the information for a read into the BOSS application.

5.1.1 Default Devices

A new BOSS site automatically contains two default devices, Manual Entries and Unassigned. A BOSS Administrator creates additional devices applicable to his/her organization.



To see the current devices in your system with information about their status:

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut.

The devices will be listed in rows with the following column headings:

Device Name – The name assigned to the device, used in the device selections and is the description of the device. The list will always include Manual Entries and Unassigned.

Name – The name that is given to the device.

Site – The group of devices to which this device belongs. Sites can be grouped by geographical location or other criteria. *See Section 5.2, Sites.*

Fixed – This box will be checked if the device is fixed camera, rather than a mobile camera.

Enabled – This box will be checked if the device is currently enabled (*see Section 5.1.4*).

Status – The Status field can display the following messages:

Device Added – If the device is newly added to the list, this message will display.

5.1.1 Default Devices *(continued)*

Offline – This device is a previously connected fixed camera that is not currently connected to BOSS.

Online Heartbeat – BOSS has detected a ping from a fixed camera.

Online Synced – The device's connection with BOSS has been established. This is shown for LPCS mobile devices only and may not change when the device is offline.

Updated – Information has been sent from BOSS to the device, and the device is up to date.

Received Logins – Updates to the device included logins that were successfully sent to the device.

Received Source – BOSS has found the hotlist source file that it needs in order to send the updated hotlist to the device. **Received Source** may not be displayed due to timing or events.

Received Hotlist – The hotlist scheduled to be successfully sent has been sent to the device.

Received Hotplates – BOSS is sending "pages" of hotplates for a large hotlist, and the last page was successfully received.

Received Targets – The update to the device included targets that were successfully sent.

5.1.2 Defining a Device

Note: Devices will be defined automatically when a 3M device, such as an ALPR camera, connects to BOSS the first time. Normally, there is no need to define devices in advance.

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. A list of existing devices will appear in the Browse/Edit area.
3. Click the **New** button.
4. Enter a name for the new device. (The name must be at least three characters long.) Note that the name **CANNOT BE CHANGED** once the device has been created.
5. Enter a **Description** for the new device. (The description must be at least three characters long.)
6. Select **Mobile** or **Fixed** in the Type field. By default, **Fixed** is selected. To change the current selection, click the **left** or **right** arrow.
7. Select a **Site**. Click the **Select** button next to the Site field to display a list of all available sites. Click on the desired site in the list and click the **Save** button.

Note: In addition to the two default sites, Manual Entries and Unassigned, which are created automatically when a new BOSS system is installed, other sites can be created by an authorized BOSS user. *See Section 5.2, Sites, for more information.*

8. Select **Owners**. Owners are groups that can access this device. For LPCS units, user logins are sent only to devices where the group is an owner of the device. Click the **Select** button next to the Owners field to display a list of all BOSS groups. Select each desired group by clicking the checkbox. When the desired groups are selected, click the **Save** button. The group name(s) selected will be displayed in the Owners field.

9. Select **Latitude** and **Longitude** values for the geographical location of a device by typing in a value or using the up and down controls on each field to increase or decrease the value. Note that some devices, such as LPCS units with a GPS attached, will automatically send the latitude and longitude of the device to BOSS.
10. Click the **Advanced** button to display additional options for the device.

    No Reads Alert – Defines how long the device must remain with no reads coming in before the system shows the device as offline.

    Alert Email – The email address or addresses to which alerts associated with this device should be sent.

    Retain Reads – The length of time that reads from this device should be saved in the BOSS database. The **Retain Reads** setting must be longer or equal to the **Retain Images** setting.

    Retain Images – The length of time that pictures captured by this device should be saved in the BOSS database.

    Retain Hits – The length of time that hits captured by this device should be saved in the BOSS database.

    SpikeStore – The 3M High Resolution ANPR/ALPR Camera P382 and the 3M Compact ANPR/ALPR Camera P372 (formerly the Spike P382 and P372 cameras) allow captured images to be stored in an on-board USB flash drive to be retrieved on demand. Setting a device as a **SpikeStore** device causes BOSS to attempt to retrieve images from the storage device when the read is requested for viewing.
11. When Advanced Options have been set as desired, click **Back** to return to the New Device screen.
12. Click the **Save** button to complete creation of the new device. The new device will now appear in the devices list above.

5.1.3 Editing a Device

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. A listing of all devices appears in the Browse/Edit area.
3. Click the desired device to select it. Details for the selected device appear in the Browse/Edit area.
4. Click the **Edit** button.
5. The Device Edit screen appears in the lower portion of the screen.
6. Modify fields as desired and click the **Save** button.

5.1.4 Enabling and Disabling a Device

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. A listing of all devices appears in the Browse/Edit area.
3. Click the desired device to select it. Details for the selected device appear in the Browse/Edit area.
4. Click the **Edit** button.
5. The Device Edit screen appears in the lower half of the screen.
6. Click the **Disable/Enable** button. The change will immediately close the edit window and return to the Devices screen. It will also take effect immediately.

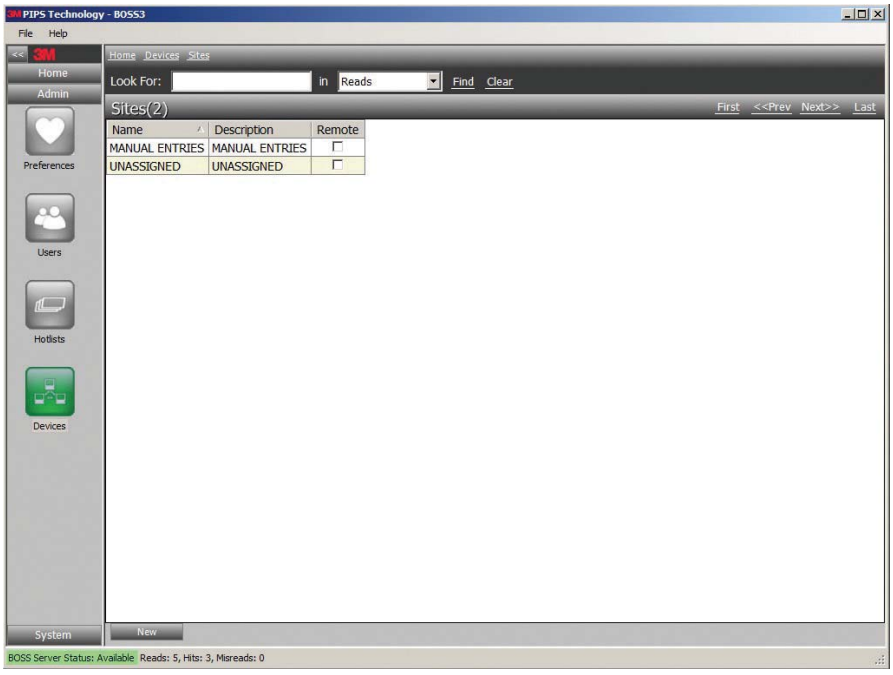
5.1.5 Deleting a Device

Note: It is strongly recommended that **devices are never deleted**. If a device is deleted, queries can no longer be performed using the device as a criterion. Instead of deleting a device, it should be disabled or given a new description.

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. (A listing of all existing devices will display in the Browse/Edit area).
3. Click the desired device in the listing.
4. Click the **Edit** button.
5. Click the **Delete** button at the bottom of the Browse/Edit area.
6. Click **Yes** to confirm the operation.

5.2 Sites

A site is a mechanism for organizing devices. This allows a BOSS Administrator to arrange devices into groups according to convenience, such as geographical area or a facility. The ability to group or arrange devices can be quite useful in large installations where there are many devices. Each device created must be assigned to a site.



5.2.1 Default Sites

A new BOSS site automatically contains two default sites, Manual Entries and Unassigned. Normally, a BOSS Administrator will want to create additional sites applicable to an organization.

5.2.2 Creating a Site

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut.
3. Click the **Sites** button at the bottom of the screen. A list of existing sites will appear in the Browse/Edit area.
4. Click the **New** button at the bottom of the screen.
5. Enter a name for the new site. (The name must be at least three characters long.) Note that the name cannot be changed once the site is created.
6. Enter a description for the site. (The description must be at least three characters long.)
7. Select the parent site for the site. BOSS allows organizing sites into tree-like hierarchies. Click the **Select** button next to the Belongs To field, and select one site from the list. Click the **Save** button to complete the selection. The site name will appear in the Belongs to field.
8. Check the **Remote** option to designate the site as a remote site. (*Remote sites are explained in Section 6, BOSS Data Sharing.*)

5.2.3 Deleting a Site

Note: It is strongly recommended that sites **are never deleted**. If a site is deleted, queries can no longer be performed using the site as a criterion. Instead of deleting a site, it is recommended that devices assigned to it should be moved to another site.

---

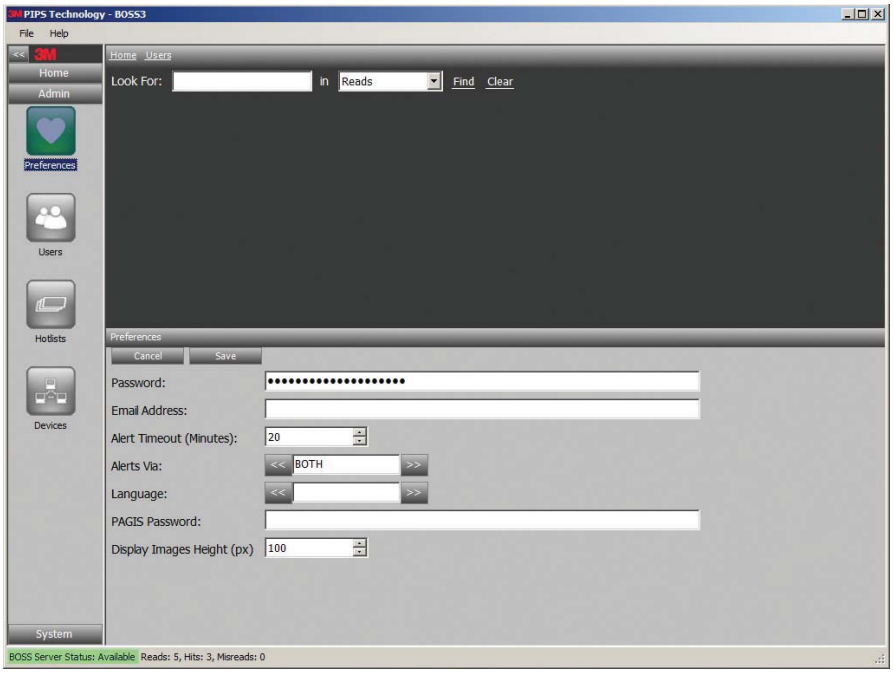
1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. A listing of all existing devices will display in the Browse/Edit area.
3. Click the **Sites** button at the bottom of the screen. A listing of existing sites will appear in the Browse/Edit area.
4. Click the desired site in the listing and click the **Edit** button.
5. Click the **Delete** button at the bottom of the Browse/Edit area. Click **Yes** to confirm the operation.

5.3 Preferences

The Preferences section allows for changing settings for the currently logged-on BOSS user, such as the password and email addresses.

5.3.1 Changing User Preferences

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Preferences** shortcut. The Preferences Entry screen appears at the bottom of the Browse/Edit area.
3. Modify the preferences settings as desired and click the **Save** button.



Password – Login password for the BOSS user. For security purposes, the existing password does not display on screen.

Email Address – Email address or addresses associated with the user. BOSS alerts for the user are sent to the email addresses specified here. Multiple addresses should be separated with a comma.

Alert Timeout (Minutes) –The cutoff time for older hits to alert the user.

Alerts Via – A user can elect to receive BOSS alerts through the Dispatch screen, emails, or both.

Language – Language preference for the user. The default value is English.

PAGIS Password (LPCS Password) – The 3M License Plate Capture Software password for the user.

Note: The user must be in a group that has been granted LPCS permissions in order for the user to log in to LPCS.

Display Images Height (px) – This setting defines the size in vertical pixels of the images (reads and hits) that will display for the user in the Dispatch and Reads Query sections.

6 BOSS Data Sharing

BOSS allows “linking” of multiple BOSS systems for data-sharing purposes. When a user issues a query from the Smart Client application that includes a remote site, the query is submitted to the local BOSS server, which in turn makes a query to the remote BOSS server(s). The combined results from all the sites are then returned to the Smart Client. ***Data from remote sites is not stored in the local BOSS server.***

The following configuration steps need to be taken to permit BOSS data sharing:

6.1 Configuring BOSS to Allow Remote BOSS Queries

1. Create a BOSS user for remote access. This user account is a “proxy” the local BOSS server will use for all requests from a remote site. This user account will have “Reads” privileges by default; no other privileges need to be given. The user must be assigned to a remote group. *(See Section 4.4, Groups, for information about flagging a group as remote.)*
2. Give the username and password for this “proxy” user to the BOSS Administrator at the remote BOSS system. The remote BOSS will need to be configured to access this BOSS system, described in the next section.

Tip: It is best to create a dedicated user account for remote sites—one that will not be used by an actual user to log in and access the application.

6.2 Configuring BOSS to Access a Remote BOSS Server

1. Obtain username and password from BOSS Administrator at the remote site.
2. Create a site for the remote BOSS server and select the **Remote** option.
3. Enter the remote site IP address and BOSS service port (23032 by default).
4. Add the username and password provided.
5. For each group that is allowed to query the remote BOSS server, assign the remote server to the user via the **Servers Access** option. *(See Section 4.4, Groups, for information on selecting Servers Access.)*
6. Log out of the application.
7. Log back on using the provided username and password. The Remote BOSS server can then be queried by selecting the desired servers in the Reads Query screen.

Note: BOSS version 3.2 and above only supports data sharing with servers running BOSS 3.0 and above.

---

7 Hotlists

A hotlist is a database that contains license plates of interest. When reads from license plate readers arrive at the BOSS server application, they are compared against hotlist records to find matches. Various hotlists can be enabled on a BOSS system and used in this comparison. In addition, hotlists can be assigned individually to specific devices. Only reads from those devices will be compared against these hotlist records. Typical hotlists include stolen vehicles, amber alerts, wants and warrants, etc. When the system reads in a plate that is determined to be a match to a hotlist entry in a hotlist, the BOSS application informs the user either with an alert sound and a pop-up window displaying a picture of the vehicle, or via email, depending on the user's preferences *(see "Alerts via" in Section 5.3, Preferences)*.

A hotlist can be a database imported from an external source, such as another law enforcement agency. It can also be a list created by the local BOSS Administrator. For the BOSS server application to be able to understand how to import the hotlist records into the database, there are three different format types that exist in a BOSS system. In addition there are several specific formats that are pre-defined and available by default when a new BOSS system is installed *(see Section 8, Hotlist Formatters)*.

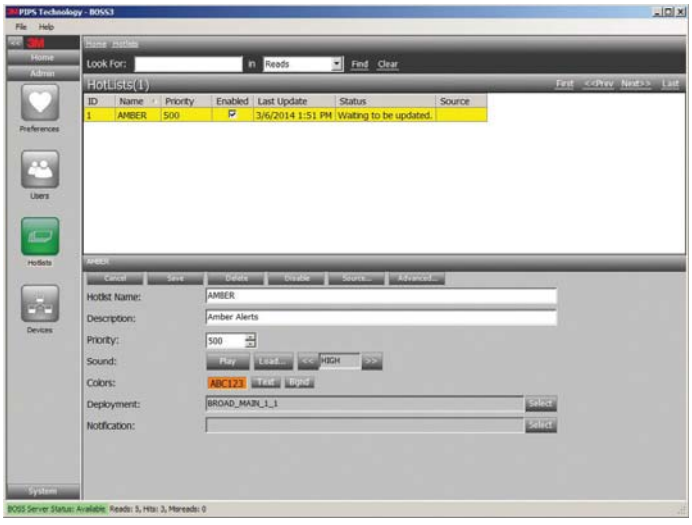
7.1 Creating a New Hotlist

There are three general areas to complete when creating a new hotlist:

- Configure basic settings.
- Define a source and provide credentials for the source (when necessary).
- Define advanced settings (optional).

7.1.1 Configuring Basic Hotlist Settings

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Hotlists** button. Currently existing Hotlists appear in the Browse/Edit area.
3. Click the **New** button at the bottom of the Browse/Edit area. The New Hotlist Entry form appears.



4. Enter a **Hotlist Name** for the hotlist. It must be at least three alphanumeric characters, and it cannot be an existing hotlist name.
5. Enter a **Description** for the hotlist (optional).

6. Select a **Priority** for the hotlist. When there are multiple hits/alerts, the priority determines which alert will occur first. (The lower the number, the higher the priority.)
7. Select a **Sound** for alerts resulting from this hotlist (optional). Click the **Load** button to select a wave sound file (*.wav). To test the selected sound, click the **Play** button. Optionally, one of the three default sounds may be selected, **Low**, **Medium**, or **High** alert.
8. Select **Colors** for the alert if desired (optional). The default is white text on a royal blue background. Custom color settings affect the entries in dispatch. The background color also applies to alerts given in LPCS.
9. Click the **Text** button to select a color for the text.
10. Click the **Bgnd** (Background) button to select a color for the background.

Note: Currently selected text and background colors are displayed in the sample box (showing “ABC123”).

---

11. Select devices for **Deployment.** Click the **Select** button to select devices from the list of those currently available. Click the checkbox next to a device in order to select it. When desired devices are checked, click the **Save** button to make the selection. One or more devices can be selected, and they will be displayed in the Deployment field.

Note: Deployment means distributing the hotlist to a device or devices. Only the devices where a hotlist is deployed will produce hits from the hotlist.

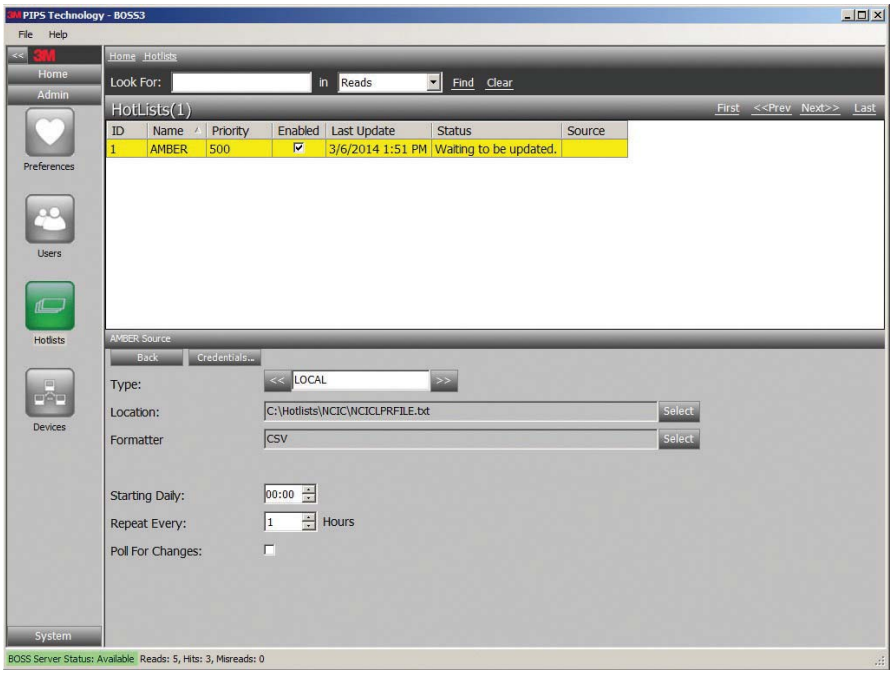
---

12. Select groups for Notification. Click the **Select** button to see a list of all BOSS groups. Click the checkbox next to a group to select the group. When you select a parent group, child groups are automatically selected. When desired groups are checked, click the **Save** button to make the selection.

Note: In order to receive alerts for hits on the hotlist, the user must be in the notification list of the hotlist. *For more information see Section 7.1.5, Defining Hotlist Advanced Options.*

7.1.2 Defining the Hotlist Data Source

1. On the New Hotlist Entry screen, click the **Source…** button to open the screen shown in the lower half of the following image:



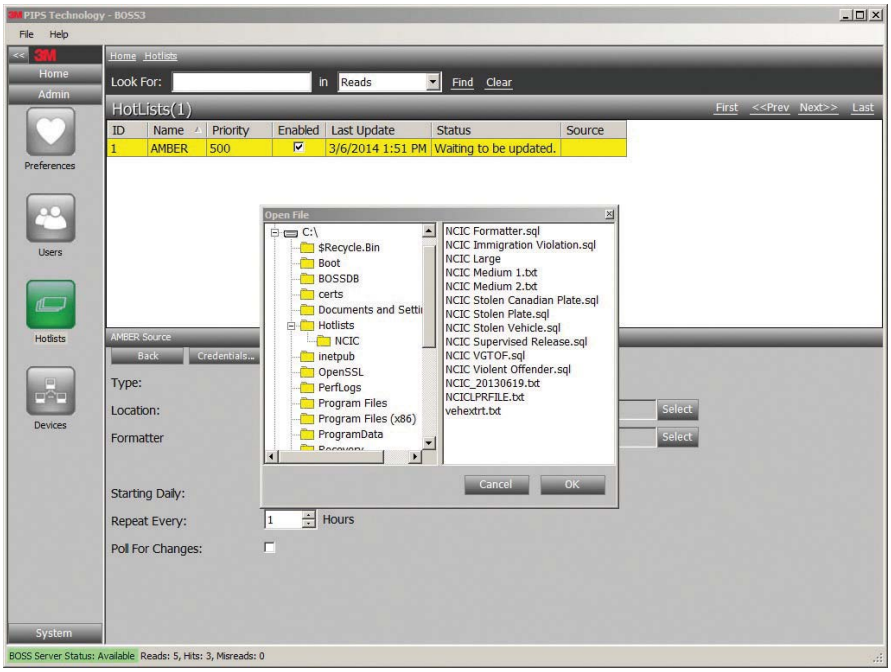
2. Choose the appropriate entries for each of the fields that describe the new hotlist:

   Type (**Network** or **Local**) – A local source means that the file is stored on the BOSS server's Windows file system. A network source means that the hotlist source resides outside the BOSS server.

Note: If a Local source is selected, the source file location (folder) must be accessible to the Windows process running the BOSS server application ("PIPS BOSS3" Windows service).

Location – Enter the location of the hotlist file. Click the **Select** button to the right of the location field.

For a local source, a file dialog will display, allowing you to navigate to a path and select a file.



For a network source, select one of the default locations displayed (if applicable), **or** type in the location of the source:

HTTP – The location format must be in Hypertext Transfer Protocol (HTTP) format: "http://server:port/path." There are a few predefined HTTP locations (such as CA DOJ) included in BOSS. These locations can be accessed with the **Select** button.

Remote BOSS System – The location format must be "boss://server:port/hotlist," where "hotlist" is the hotlist name on the remote system.

Note: The remote system hotlist name **MUST** be alphanumeric and **CANNOT** contain any spaces.

Formatter – Formatter defines the way a hotlist database file is parsed into discrete fields. Click the **Select** button next to the Formatter field. A list of available formatters appears. Click on the desired formatter and click the **Save** button to make the selection. The name of the selected formatter will appear in the field.

Note: Normally one of the several default formatters included with BOSS is sufficient. A new custom formatter can be created if necessary. *See Section 8.1, Creating a New Formatter for Hotlists, for more information.*

7.1.2 Defining the Hotlist Data Source *(continued)*

Starting Daily – Specify the time of day the hotlist should begin updating each day. The time is formatted as hours:minutes in the 24-hour clock, i.e., between 00:00 and 24:00 can be selected.

Repeat Every – Specify the time interval, in hours (1 – 24), between updates.

OR

Poll for Changes – If you choose this setting, BOSS will check for updates to the hotlist approximately every 30 seconds. When this option is selected, the **Starting Daily** and **Repeat Every** options are disabled.

Note: If **Poll for Changes** is selected, and the hotlist source resides on the network, BOSS will attempt to make a network connection every 30 seconds. This frequency may add significantly to network traffic. Use with caution.

7.1.3 ZIP Compressed Hotlist Files

BOSS will automatically recognize and extract a hotlist data file contained in a ZIP archive file, such as Windows Explorer compressed (zipped) folder.

Note: There can be only one file in the ZIP archive.

7.1.4 Defining Hotlist Source Credentials

Some sources will require credential settings (e.g., login information) in order to allow BOSS to access that data. To enter the Credentials Settings screen from the Hotlist Source screen, click the **Credentials** button.

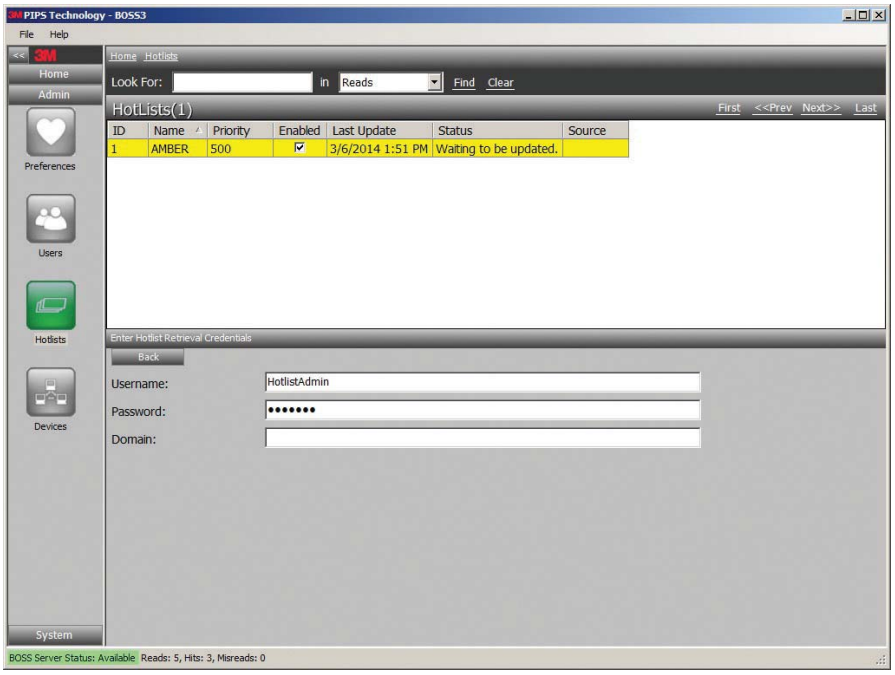
The credentials depend on the source type as follows:

Network-HTTP – If the HTTP (website) source defined requires login information, it should be entered in the Credentials Setting screen. This information will include username and password. The domain field may be necessary as well. Consult the Administrator of the HTTP source for required login information.

Network-Remote BOSS system – A username and password valid on the remote BOSS system must be entered (as in remote sites configuration, described in Section 6.0, BOSS Data Sharing). Consult the Administrator of the remote BOSS system for a username and password.

To set credentials for a source:

1. Click the **Credentials** button. The Credential Input screen appears.
2. Enter the username, password, and domain information applicable to the source you are specifying.
3. Click the **Back** button to return to the Source Entry form.
4. Click the **Back** button again to return to the New Hotlist Entry screen.



7.1.5 Defining Hotlist Advanced Options

Advanced Options are values that allow you to further define details of the new Hotlist. To access the Advanced Options, click the **Advanced…** button.

Covert – A covert hotlist is one that contains sensitive information that should only be available to certain user groups.

The effects of defining a hotlist as covert are as follows:

- A hit on the covert hotlist will not be alerted to users in mobile LPCS vehicles, unless the logged-on user is a LPCS Administrator.
- A hit on the covert hotlist will not be alerted in the BOSS application, regardless of the user alert preferences. Hit alerts for covert hotlists will be sent only via email.
- When reads are queried, hit information on covert hotlists will be displayed only to users in the Notifications list for the hotlist. Other users will see that the read is a hit, but no information will be shown.
- Hit information for hits from covert hotlists will not be sent to remote BOSS servers.

Whitelist – This option, when selected, defines the hotlist to be a whitelist, which works in reverse to a normal hotlist. A whitelist defines a list of plates that are **authorized** and not of concern. When a whitelist is active, license plates read that do ***not*** match an entry on the list will trigger a hit/alert.

7.1.5 Defining Hotlist Advanced Options *(continued)*

An example of whitelist use might be a secure parking lot where fixed camera devices are monitoring vehicles entering. Authorized plates will match entries in a whitelist hotlist. If a plate is read that does not match an entry in the whitelist, an alert occurs.

Whitelists and hotlists can be active simultaneously for a device.

Note: Whitelist support in LPCS requires a separate license. If you do not have the license and wish to use whitelists, please contact your 3M sales representative for further information.

Ext Trigger – This option, when selected, sets the External Trigger flag on a hotlist when it is passed to LPCS. It is only supported in LPCS version 2.6.6 or above and will have no effect on earlier versions of the software.

One Time – This option, when selected, specifies that the hotlist data should only be accessed from its defined source one time; no subsequent updating will occur after the initial import.

Alert Timeout – This setting allows you to define how current a hit (from this hotlist) must be in order to cause an alert. This primarily pertains to information coming in from mobile units, where there may be a large delay. Alert Timeout can be specified in minutes, hours, days, or months.

Delete Inactive – BOSS updates hotlists in an incremental manner, and instead of deleting hotlist entries that no longer exist, non-existent entries are marked as "inactive." If the entry subsequently becomes valid, the entry is marked as active again. The Delete Inactive value determines how long inactive entries are kept in the BOSS hotlist database.

Note: If LPCS mobile units are used, this value should be set to the longest time between begin shift downloads to LPCS.

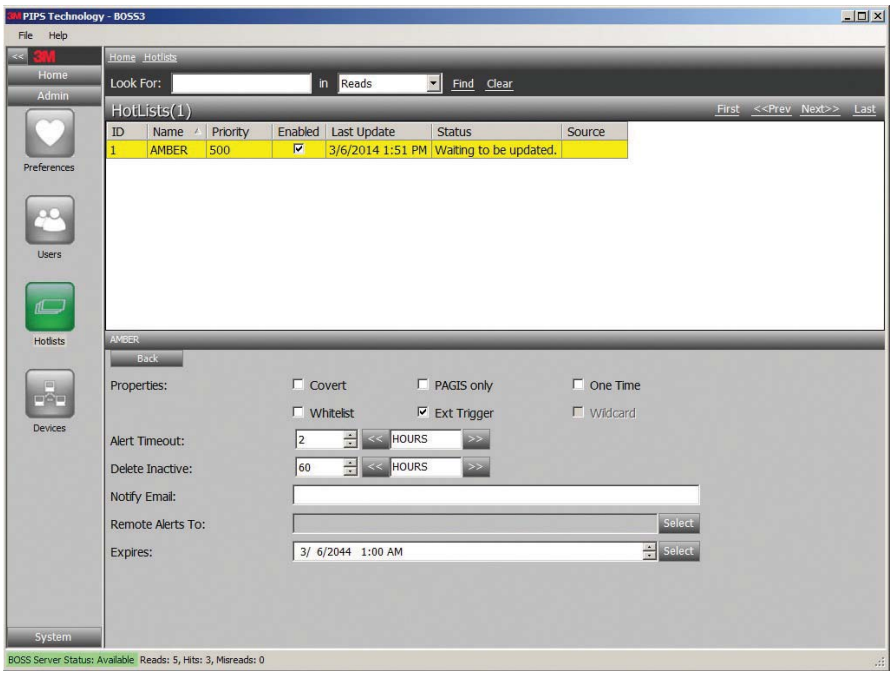
Notify Email – One or multiple email addresses may be defined to receive an alert when there is a hit. Multiple email addresses can be entered in the field, separated by a comma.

Remote Alerts To – Select the remote sites in which to send alerts. When a BOSS system sends an alert to a remote system, it is sent as a read; the remote BOSS system then determines whether to treat the read as a hit.

Note: This setting is only applicable if remote sites are defined.

Expires – Determines the date that the hotlist will stop importing data from its source. For a hotlist that is intended to be permanent, leave the expiration at the default value, 30 years from current date.

7.2 Enabling and Disabling a Hotlist



1. Select the **Admin** category on the Shortcut bar.
2. Click the **Hotlists** shortcut. A list of all hotlists appears in the Browse/Edit area.
3. Click the desired hotlist. Details for the selected hotlist appear in the Browse/Edit area.
4. Click the **Edit** button.
5. The Hotlist Edit screen appears in the lower half of the screen.
6. Click the **Disable** or **Enable** button.

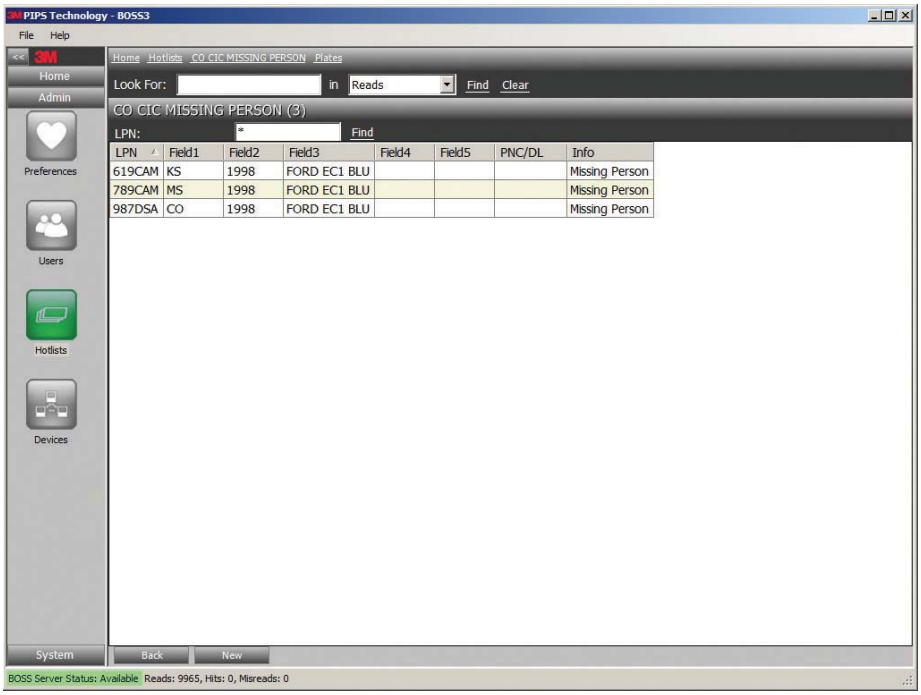
7.3 Modifying Hotlist Entries

BOSS allows viewing, adding, editing, and deleting hotlist entries.

Note: If the hotlist is set to update automatically, any changes to that hotlist made from within the BOSS User Interface application will be lost at the next automatic update.

7.3.1 Querying Hotlist Entries

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Hotlists** shortcut. A listing of all hotlists appears in the Browse/Edit area.
3. Click the desired hotlist. Details for the selected hotlist appear in the Browse/Edit area.
4. Click the **Plates** button.
5. The Hotlist Plates screen will be displayed.

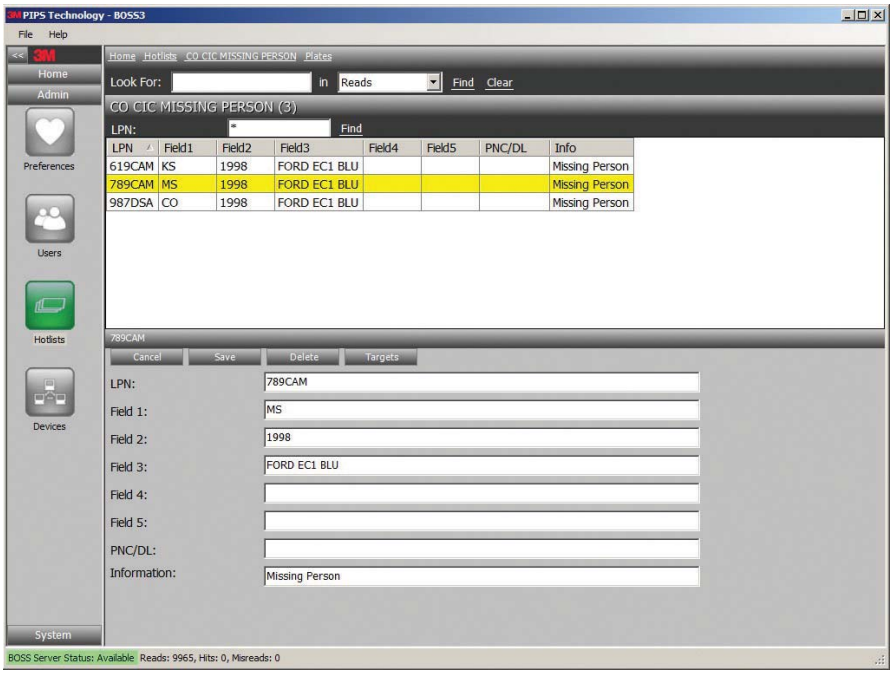


6. Type in the full or partial plate text to search for in the LPN field. (Wildcard searches are supported. *See Section 11.1, Wildcards, for more information.)*
7. Click on **Find**. License plates that match the criteria will be displayed. Note that only the first 1,000 matching license plates will be shown.

7.3.2 Editing a Hotlist Entry

1. Retrieve hotlist plates as instructed in the previous section.
2. Click on the row showing the desired plate.
3. The Plate Edit form will be displayed at the bottom of the screen.
4. Edit the field values as desired.
5. Click **Save** to save changes.

Note: Manually edited hotlist entries will be lost the next time the hotlist is updated.



7.3.3 Adding a Hotlist Entry Manually

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Hotlists** shortcut. A listing of all hotlists appears in the Browse/Edit area.
3. Click the desired hotlist to select. Details for the selected hotlist appear in the Browse/Edit area.
4. Click the **Plates** button.
5. Click the **New** button. The Plate Edit form will be displayed at the bottom of the screen.
6. Enter the **LPN** (mandatory) and other fields (optional).
7. Click **Save** to save changes.

Note: Manually added hotlist entries will be lost the next time the hotlist is updated.

7.3.4 Deleting a Hotlist Entry

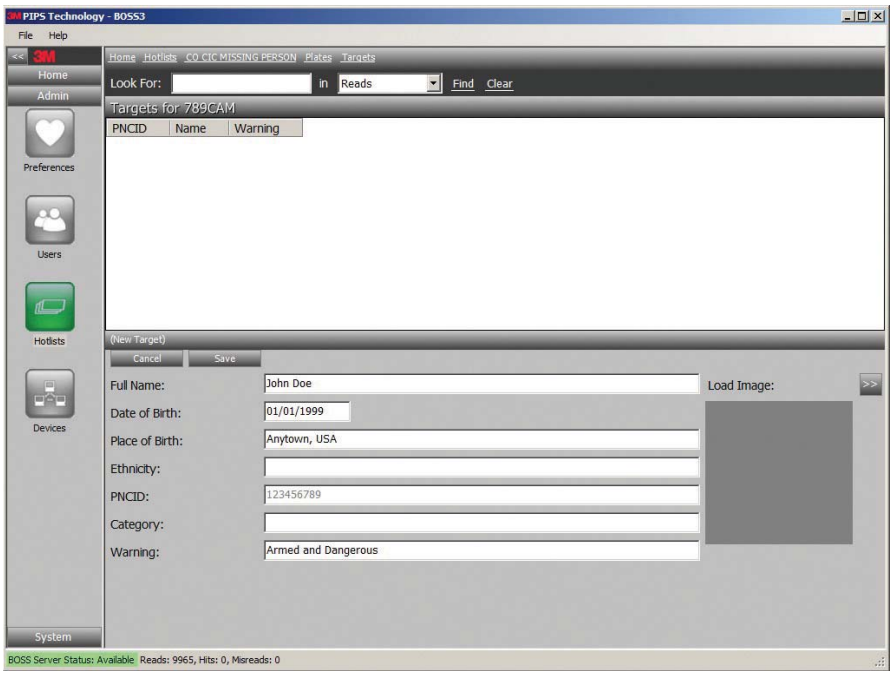
1. Retrieve hotlist plates as instructed in the Querying Hotlists Entries section.
2. Click on the row showing the desired plate. The Plate Edit form will be displayed at the bottom of the screen.
3. Click the **Delete** button.
4. Click **Yes** to confirm the deletion.

Note: Manually deleted hotlist entries may be re-added the next time the hotlist is updated.

7.4 Targets

Targets are individuals of interest associated with a license plate. Target information is downloaded to the LPCS mobile application from BOSS.

1. Retrieve hotlist plates as instructed in Section 7.3.1, Querying Hotlists Entries.
2. Click on the row showing the desired plate.
3. The Plate Edit form will be displayed at the bottom of the screen.
4. Click the **Targets** button. Information about the target will display.



7.4.1 Creating a New Target

1. Click the **New** button.
2. The Target Edit form will be displayed.
3. Fill in the fields, listed below, with appropriate values.

   Full Name – The first and last name of the target.

   Date of Birth – The date of birth of the target.

   Place of Birth – The location where the target was born.

   Ethnicity – The ethnicity (race or national origin) of the target.

   PNCID – This field can be used to enter any type of identification number that is available. In the UK this is the Police National Computer identification number of the target. This field is linked to the PNCID field in the hotlist information in the LPCS application. *See the sample INI configuration file in Section 5 of the 3M License Plate Capture Software User's Manual.*

   Category – The category of the target, such as Felon, Suspect, etc.

   Warning – The warning information to display to the officer.

   Load Image – An image of the target, such as a DMV photo or "mugshot," can also be associated with the Target record. Upload an image by clicking on the **Select** button and browsing to the image file. Supported formats include JPG, GIF, or BMP.
4. Click the **Save** button.

7.4.2 Deleting a Target

1. Access the Targets screen as described above.
2. Click the row containing the target to be deleted.
3. The Target Edit form will be displayed.
4. Click the **Delete** button.
5. Click **Yes** to confirm deletion.

8 Hotlist Formatters

Hotlist Formatters define the structure of source data that is imported into BOSS Hotlists. BOSS includes several default formatters when the software is installed. There are three types of formatters:

CSV (comma-separated values) – A flat text file containing one line for every record. Each field in the record is separated by a comma.

Fixed Length – A flat text file containing records that are all the same length. No separator characters are used to determine where each field ends and another begins, but rather, field and record lengths are known up front. In a fixed length file, padding spaces are used where necessary, to accomplish the correct field length.

NCIC (United States National Crime Information Center) – The NCIC database is a computerized index of criminal justice information (i.e., criminal record history information, fugitives, stolen properties, missing persons, etc.), that is available to law enforcement agencies 24 hours a day, 365 days a year. Several NCIC import sources/formats exist within BOSS.

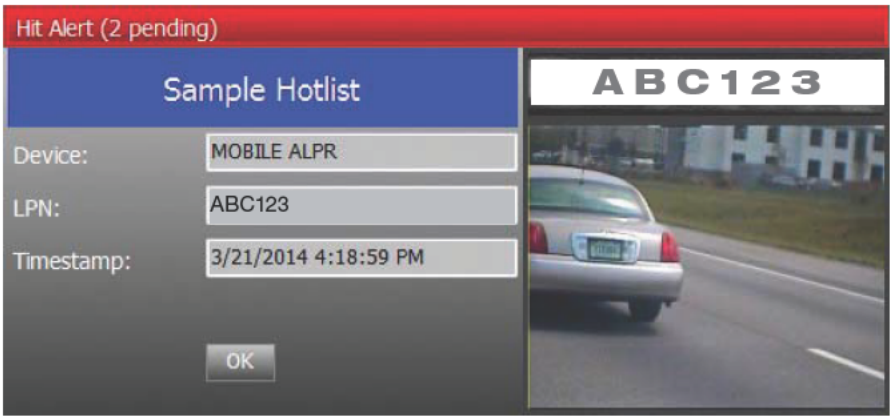
8.1 Creating a New Formatter for Hotlists

Normally, when creating a new hotlist, you will find that one of the default formatters can be used. However, BOSS does give you the flexibility to create new hotlist formatters. Creating a new formatter or modifying an existing formatter should be approached with caution and is beyond the scope of this manual. 3M provides BOSS training that details creating and modifying hotlist formatters in practice. *For more information, please contact 3M Technical Support.*

9 Alerts

BOSS can provide real-time alerts on-screen, via the BOSS User Interface application, or through email. In order to receive alerts through the BOSS application, **the logged-on user must be in a group that is assigned the Dispatch permission**. Email alerts can be sent to any BOSS user or email recipient.

A real-time alert for a hit can pop up on the screen at any time when the BOSS application is running, regardless of which screen the user has active. A sound associated with the hit will be played. Alerts will be queued until the user acknowledges them by clicking **OK**. Real-time alerting in the BOSS application can be turned off by clicking on the **Alerts** toggle button on the BOSS Home screen. The settings for real-time alerts can be modified through the Dispatch screen, *(see Section 10, Dispatch)*.



10 Dispatch

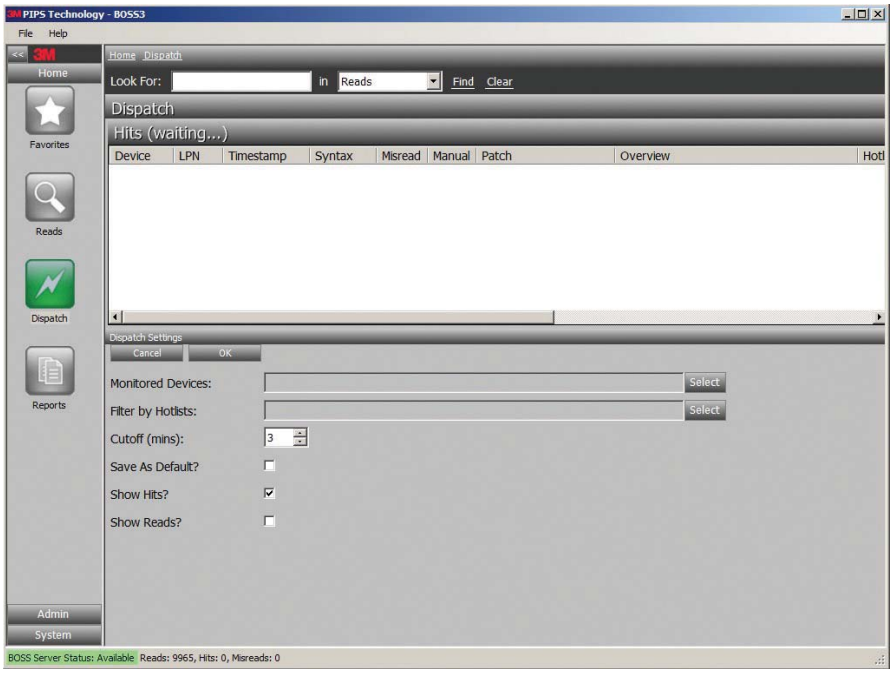
The Dispatch screen is a tool often used by first responder dispatchers. It enables them to easily view hits, monitor reads, and correct license plates as they enter the BOSS system. The information displayed is as near to real time as possible. For ease of viewing, there are three configurations that can be set:

- If only the hits are set to display, they will appear on the whole screen.
- Similarly, if only the reads are set to display, they will appear on the whole screen.
- If the dispatcher is monitoring both hits and reads, then the hits will be displayed on the top half of the screen and the reads will be displayed on the bottom half.

10.1 Dispatch Settings

Dispatch Settings allow you to choose the information shown on the Dispatch screen.

1. Select the **Home** category in the Shortcut bar.
2. Click the **Dispatch** shortcut.
3. Click the **Settings** button in the bottom of the Browse/Edit area.



4. The following settings are available on the Dispatch screen. Change these settings as desired:

   Monitored Devices – Camera sources can be selected or deselected from a pick list to control which ones will supply reads (and resulting hits) to the Dispatch screen. Individual dispatchers can focus on particular camera inputs by selecting/deselecting any combination of sources (one, multiple, or all) for monitoring.

   In large BOSS systems, it may not be practical for a single dispatcher to monitor all sources simultaneously. An organization may choose to assign individual dispatcher personnel to different sources or may select to focus on particular sources during certain time periods or events.

Filter by Hotlists – Hotlists may be selected to only show hits from designated hotlists. If there are no hotlists selected, hits from the monitored devices will be displayed.

Cutoff (mins) – The cutoff setting determines how current from the present time a hit or read must be in order to display on the dispatch screen This setting determines the number of minutes before data is discarded from the on-screen display. The maximum time is 10 minutes.

Save As Default – If checked, the current settings are saved and restored the next time the user logs in. Note that selected devices will always default to the devices where the user is configured to receive notifications in the Hotlist settings. *See additional information on notifications in Section 7.1.1, Configuring Basic Hotlist Settings.*

Show Hits? – If checked, hits will display in rows in the top section of the Dispatch screen as they occur. If this option is deselected, rows of hits are not displayed in this section of the Dispatch screen. However, pop-up alerts will still display for hits, regardless of this setting.

Note: If the **Alert Toggle** button is set to the **Off** position, hits and reads will not display in the Dispatch screen. *See Section 9, Alerts, for additional information.*

Show Reads? – If checked, all reads included in the devices selected in the Monitored Devices field display in the dispatch screen. By default, this option is not selected.

Note: Monitoring reads may slow down the BOSS server. It is recommended that reads are only monitored for diagnostics purposes.

---

5. Click the **Save** button for the changes to take effect.

10.2 Dispatch Hits

For each row, the columns displayed are:

Device – The device where the read originated.

LPN – The license plate characters read in by a camera or manually entered by a user.

Timestamp – Date and time when the read occurred.

Syntax – The state or region of the plate, if available.

Misread – If checked, indicates that the hit resulted from a read that was marked as a misread.

Manual – If checked, indicates that the hit resulted from a manual entry (put in by a BOSS user).

Patch – A thumbnail image of the license plate.

Overview – Color overview picture of the vehicle.

Hotlist – The name of the hotlist from which the hit occurred.

Field1 … Field5 – Fields originating from the hotlist. The content and meaning of these fields vary depending on the composition of the hotlist.

PNC/DL – This field can be used for a driver's license (DL) number in US installations, but primarily used in United Kingdom installations for storing the UK Police National Computer identification number.

10.2 Dispatch Hits *(continued)*

Info – Commonly contains additional text associated with the hit record. When the hotlist source contains additional fields, the information from those fields is all stored in this one field.

Priority – Priority assigned to the hotlist, with a lower number being given a higher priority.

Annotation – Notes associated with the read. Annotations are entered by BOSS users.

10.3 Dispatch Reads

For each row, the columns displayed are:

Device – The device where the read originated.

LPN – The license plate characters read in by a camera or manually entered by a user.

Syntax – The state or region of the plate, if available.

Timestamp – The date and time when the read occurred.

Patch – A thumbnail image of the license plate.

Overview – Color overview image of the vehicle.

Misread – If checked, indicates that this record was marked as a misread.

Hit – If checked, indicates this read resulted in a hit.

Manual – If checked, indicates this read was input manually by a BOSS user, rather than originating from a device.

Annotation – Notes associated with the read. Annotations are entered by BOSS users.

10.4 Manual Entries

There may be times when a read must be manually entered or when a camera does not correctly read a plate. For example, if there was an obstruction between the camera and the plate, then characters may be missed in the read. For this reasons, manual entries can be completed by an authorized user via the Dispatch screen.

10.4.1 Adding a Manual Read

1. From the Dispatch screen, click the **Add** button. The Manual Entry screen appears in the lower half of the Browse/Edit area.

Note: The **Add** button will only be present if the logged in user has the Edit Access permission to reads.

---

2. Enter the plate characters in the LPN field.
3. Click the **Select** button to the right of the disposition field.
4. Select the desired disposition(s) and click the **Save** button to complete the selection.
5. Click the **Save** button to finish saving the manual entry. If the “Manual Entries” device is not being monitored, the manual entry will not appear in the Dispatch screen.

10.4.2 Correcting Reads

1. In the Dispatch screen, double-click on the read to be corrected. The Manual Entry screen appears in the lower half of the Browse/Edit area.
2. Enter the plate characters in the LPN field.
3. Click the **Select** button to the right of the disposition field.
4. Select the desired disposition(s) and click the **Save** button to complete the selection.
5. Click the **Save** button to finish saving the corrected entry.

11 Querying Stored Data

The Reads screen allows for searching and viewing past read records on a local server or on a remote server that has granted access. Reads can be quickly searched by entering a license plate number. This screen also allows for more advanced queries where data can be filtered based on additional fields such as date ranges, location, and radius. Additionally, the Reads screen allows you to perform multiple queries with the use of tabs.

For the queried results returned, there are no limits to the number returned from a local server. To limit the impact on outside systems, there is a limit of 1,000 records returned from a remote server. A maximum of 1000 records will be displayed per page.

Note: Depending on factors such as the size of the BOSS database, the speed of the server, the bandwidth of the connection between client and server, and the parameters of the query, there may be a delay before the results are displayed. A status bar will display that shows that the query progress.

11.1 Wildcards

Wildcards are special characters that represent any alphanumeric character and can be used in searches and queries. Wildcards can make finding a match easier because they can define a portion of the criteria to be ambiguous. Wildcards supported in BOSS are described in the following table.

WILDCARD USED	REPRESENTS
a%	Any values that start with the letter “a”
a	Any values containing “a”
% or *	Any/all values
a_	Any values that are exactly two characters long and start with “a”
_a*b	Any values that have “a” as the second letter and end with “b”
[abc]*	Any values that start with “a”, “b” or “c”

11.2 Quick Search Bar

The Quick Search bar is always visible and available on the top of the BOSS screen regardless of the category or shortcut currently selected. This feature allows for quick, simple searches of various BOSS data.

1. Type the value to search for in the Look For field. This value can include wildcard characters. Multiple values can be entered separated by a comma (e.g., ABC123, XYZ234). However, wildcard values cannot be used when searching for multiple values.
2. In the “In” drop-down box select an area to search. The available options are **Reads**, **Hotlists**, **Users**, **Group Users**, **Groups**, **Devices**, and **Sites**. These areas are described below.
3. Click the **Find** link to initiate the search. The results will be displayed in the Browse/Edit area of the screen.

11.2.1 Quick Search Fields

When performing a query using the quick search feature, keep in mind that the search is performed in one significant area that can be selected. The search is then run against the significant field in that area, not all fields in that area. For example, when performing a quick

search in Users, the text entered is compared against the Username field of all user records. However, it is not compared to the display names for users. The following is a list of the fields used in the Quick Search:

SEARCH IN AREA	FIELD USED FOR SEARCH
Reads	LPN
Users	Username
Groups	Group Name
Site	Site Name
Hotlists	Hotlist Name
Group Users	Group Name
Devices	Device Name

11.3 Query Result Navigation Icons

Just above the query results are navigation icons that facilitate moving through the data results. These icons can be very useful for larger result sets, providing an easy way to move through records.



Move to the very beginning of the data results, i.e., the first record.



Move backward through the data results.



Move forward through the data results.



Move the very end of the data results, i.e., the last record.

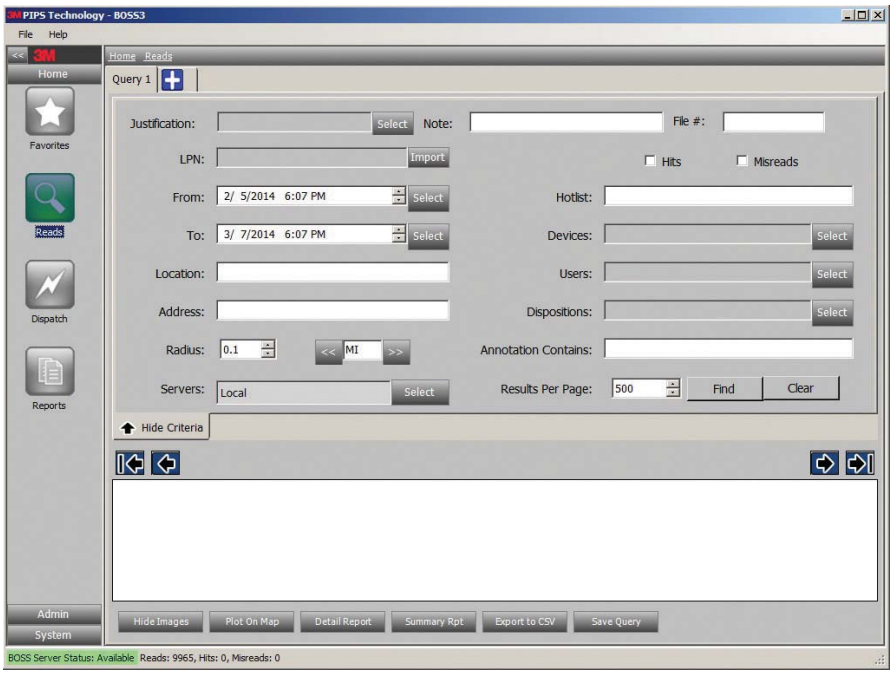
11.4 Advanced Reads Queries

The Reads screen allows for searching and viewing past read records. Reads can be quickly searched by entering a license plate number. The Reads screen also allows for more advanced read queries where data can be filtered based on additional fields such as date ranges, location, or radius. As indicated earlier, a maximum of 1000 records will be displayed.

11.4.1 Performing an Advanced Reads Query

1. Select the **Home** category on the Shortcut bar.
2. Click the **Reads** shortcut.
3. Enter desired query criteria *(see the following section, 11.4.2, Entering Advanced Reads Query Criteria)*. All fields do not have to be filled in. Leaving a query field blank simply means there will be no filtering on that field.
4. Click the **Find** button to run the query.

11.4.2 Entering Advanced Reads Query Criteria



The query criteria fields are:

LPN – Full or partial (using wildcards) license plate number.

From – The start date and time for reads to be retrieved. Either click the **Select** button to display a calendar for quick selection, or type in the date.

To – The end date and time for reads to be retrieved. Either click the **Select** button to display a calendar for quick selection, or type in the date.

Location – The location as entered in the LPCS application *(see the 3M License Plate Capture Software User's Manual for more information)*.

Near Address – An address to use as the center of a radius search. The address format depends on the mapping system used but typically street name, house number, city and state, or zip code can be entered.

Radius – When a Near Address filter is entered, the search radius from the center point **must be** entered here.

Servers – Information can be queried from one or more remote BOSS servers. Click the **Select** button to display a list of authorized BOSS servers.

Justifications – Select the justification that best describes the purpose for the query being performed. This field will only be displayed if Justifications have been enabled in the System Parameters. *See Sections 15.3.2, List of BOSS System Parameters, and 15.7, Justifications, for more information.*

Justification Note – Enter any additional information necessary to more accurately document the query being performed. This field will only be displayed if Justifications have been enabled in the System Parameters. *See Sections 15.3.2, List of BOSS System Parameters, and 15.7, Justifications, for more information.*

Hits Only – If checked, only hits are queried.

Misreads Only – If checked, only reads that are marked as misreads are queried.

Hotlist – A search on hits can be limited to a specific hotlist, which can be entered here.

Devices – A query can be narrowed to reads originating from a particular device. Click the **Select** button to display a list of devices, select one or more.

Users – A query can be narrowed to reads originating by a particular user. Click the **Select** button to display a list of users and select one or more.

Note: The username can also be typed in.

Dispositions – A query can be narrowed to reads with a particular disposition. Click the **Select** button to display a list of dispositions. Then select one or more dispositions.

Annotation Contains – If text is entered in this field, only reads that contain the text in the annotation field are queried.

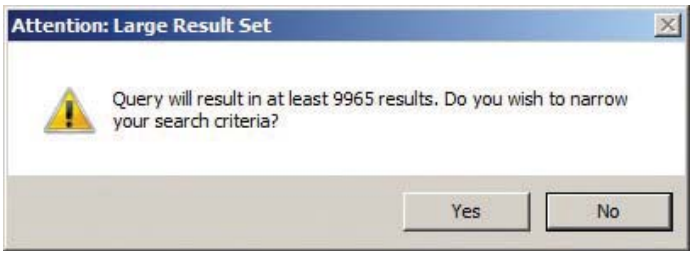
Results Per Page – The maximum number of reads that will be displayed. The default is 500, the maximum is 1,000.

Clear – If clicked, the fields on the current tab will be returned to their default values.

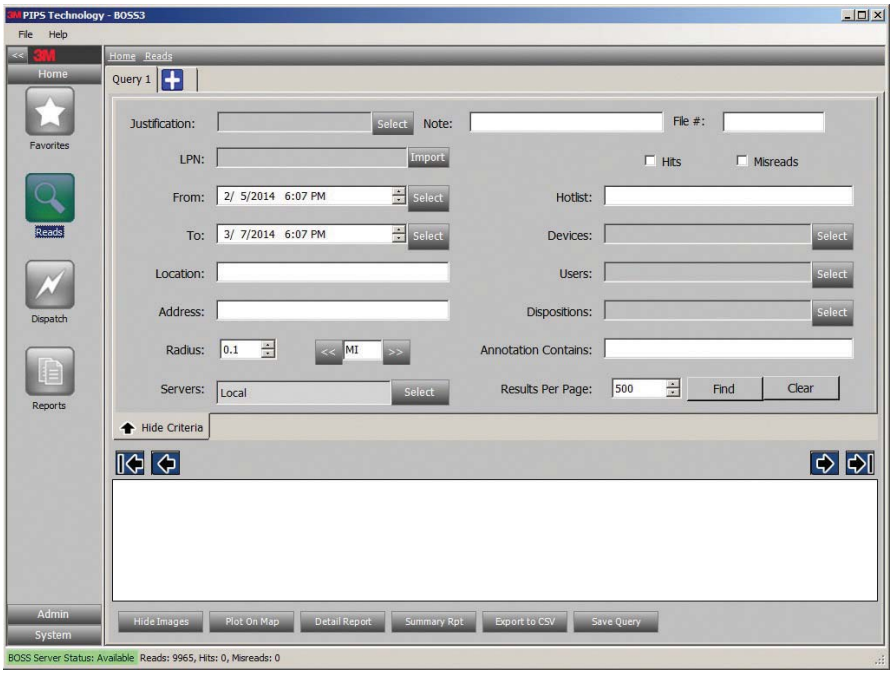
11.4.3 Managing Query Results

With the ability to obtain any number of results from a local server comes the option to narrow the potential results to be returned. If a large number of results will be returned based on the criteria entered, a message is displayed asking if the search criteria should be narrowed. If you select **Yes**, the search criteria is redisplayed offering the chance to make any necessary changes to reduce the results. If you select **No**, the query is performed based on the current criteria selections.

Note: A large number of results can take several minutes to be displayed.



11.5 Multiple Query Tabs



With Query tabs, users can perform multiple queries at a time. By clicking on the last tab, which contains the plus icon, you can access additional Reads Query screens. Enter the desired search criteria on each new screen to obtain additional information through the varying results. Each query can be given a descriptive name by right-clicking on the tab, and obsolete queries can be removed the same way.

11.6 Cross-Referencing External Data

BOSS allows cross-referencing external data, such as DMV information. To query BOSS based on external information, take the following steps:

1. Create a CSV text file containing the license plate numbers to be cross-referenced. **The license plate number must be in the first field.**
2. Open the Reads Query screen.
3. Click the **Import** button next to the LPN field.



4. Click **Open** to import the plate numbers. A maximum of 50 plate numbers can be referenced at a time. Imported plate numbers will show up in the LPN field:



5. Enter other query criteria, as needed, and click **Find** to run the query.

11.7 Working with Queried Reads

11.7.1 Viewing Query Results

The results of both Quick Searches and Advanced Reads Queries are presented in the same manner.



The columns displayed are:

LPN – The plate text (characters) read in by a camera or manually entered by a user.

Timestamp – The date and time when the read occurred.

Patch – A thumbnail image of the license plate.

Overview – The color overview picture of the vehicle.

Device – The device where the read originated.

Site – The site where the read originated.

Misread – Indicates whether the read was marked as a misread by a user.

Hit – Indicates whether the read is a hit.

Manual – Indicates whether the read was entered manually.

Login – The username logged into the device at the time the read originated.

Location – The location entered in the LPCS system. *See the 3M License Plate Capture Software User's Manual for more information.*

Latitude – The latitude coordinate of the device at the time the read originated.

Longitude – The longitude coordinate of the device at the time the read was originated.

Hotlist – The name of the hotlist that produced the hit.

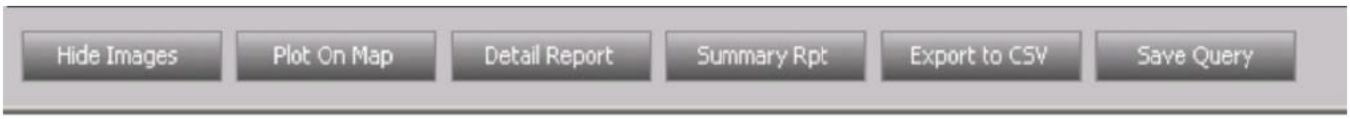
Field1 … Field5, PCNID, Information – Information from the hotlist that produced the hit.

Annotation – Annotations entered for the read.

Server – The name of the server that has provided this information. This can be a local or remote server.

11.7.2 Query Results Actions

There are several button options available at the bottom of the Reads Query Results screen that offers additional uses of the data results.



Hide Images/Show Images – Used to remove the image columns, patch and overview, from the view. This can be done to provide more room for text fields to be displayed. When clicked, the **Hide Images** button's caption changes to **Show Images.** When the button is clicked again, images will again be displayed.

Plot On Map – When clicked, any selected records will be plotted on a map. One or multiple records can be selected by clicking the checkbox in the first column of the record. To select all of the records, click the checkbox in the headings column.

Detail Report – Click to generate a detailed report of selected reads. To select one or more records, click the checkbox in the first column of the record. To select all of the records on the current page, click the checkbox in the headings column. Use the navigation buttons to move to additional pages to select additional records.

Summary Rpt – Click to get a summary report of selected reads. To select one or more records, click the checkbox in the first column of the record. To select all of the records on the current page, click the checkbox in the headings column. Use the navigation buttons to move to additional pages to select additional records. To include all results choose the **All Results** option in the Reads Summary Detail Report option box.

Export to CSV – Click to save the results to a file in a CSV format. Select to save the current page or all results provided. Use the navigation buttons to move to additional pages to select additional records.

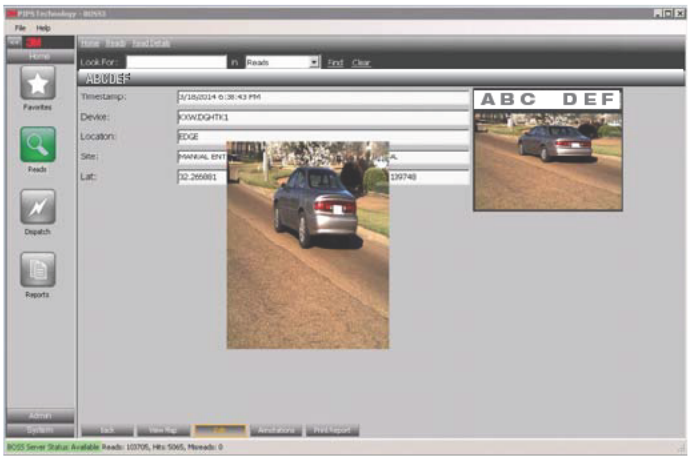
Save Query – Click to save the query criteria as a favorite for future use. *See Section 11.8, Favorites, for more information.*

11.7.3 Viewing Read Details

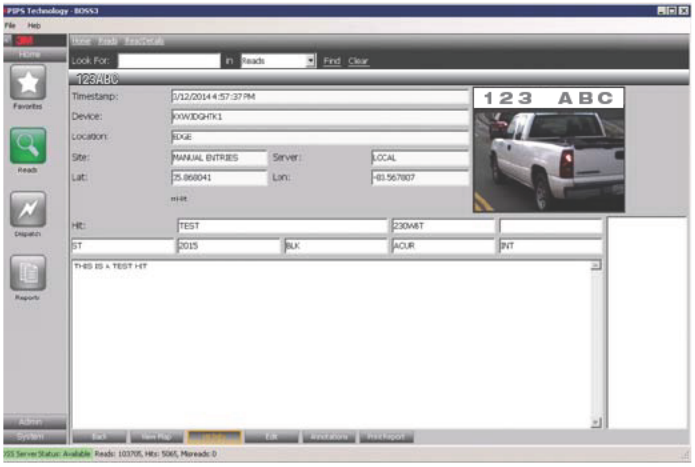
Click a row in the query results to view the details of the record.



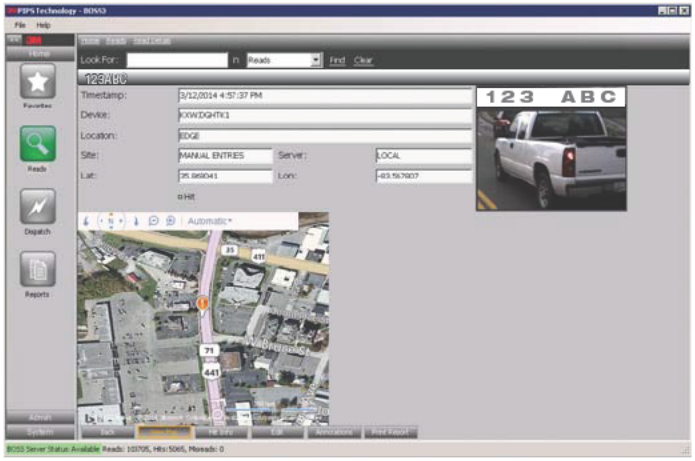
The Read Details screen displays the license plate text in the title. The timestamp, originating device, site, and geographical coordinates are displayed below. The plate patch and vehicle color overview images are on the right.



The vehicle color overview picture can be enlarged by clicking on the picture. Use a mouse scroll wheel or the cursor up and down keys to resize the image. Left-click on the enlarged image to close. Right-click on the image to copy the image to the Windows Clipboard.

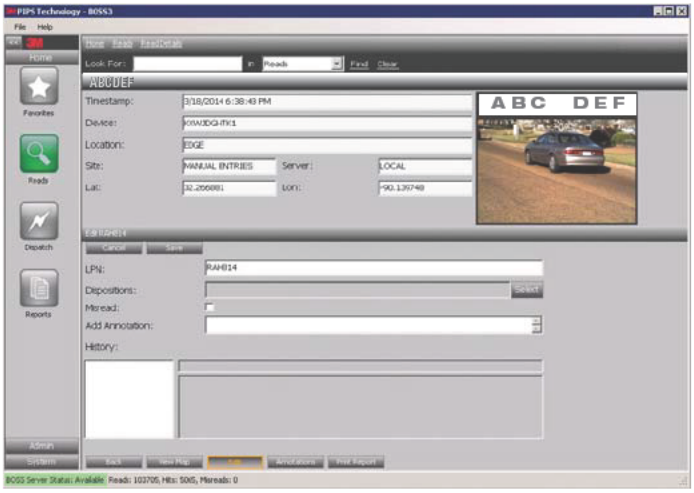


If the read is a hit, details of the hit can be displayed by clicking on the **Hit Info** button at the bottom of the screen.



A map plotting the location where the read occurred can be displayed by clicking on the **View Map** button.

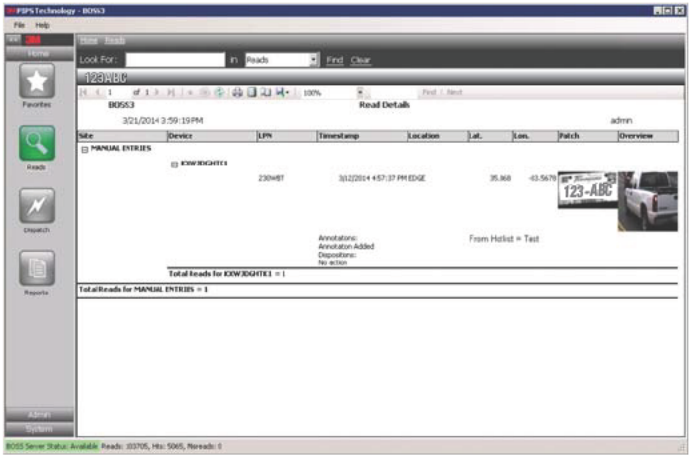
11.7.3 Viewing Read Details *(continued)*



Use the **Edit** button to correct the plate text and/or assign a disposition and annotation to the read. Click on **Save** to save the changes. The plate text can also be marked as misread if the read information is found to be incorrect.



Annotations associated with the read can be viewed by clicking on the **Annotations** button.



A report containing the read's details can be printed by clicking on the **Print Report** button.

11.8 Favorites

Favorites are read queries that use specified criteria, which have been saved. Favorites can be reused, which allows the user to quickly perform frequently needed queries without having to define the parameters each time. Favorites are specific to each user.

11.8.1 Creating a New Favorite

1. Select **Home** on the Shortcut bar to access its icons.
2. Click on the **Read** shortcut.
3. Enter the desired query parameters in the Browse/Edit area (e.g., data range, location, radius, servers).
4. Click the **Go** button to run the query.
5. When the query results window appears, click the **Save Query** button.
6. A dialog box will appear, prompting for a name. Enter a descriptive name for the new favorite.
7. Select the **Use Relative Date Range** option if desired.

   Use Relative Date Range Option – If this option is selected when saving a query, and when the resulting favorite query is run in the future, it will use a From and To date and time range relative to the From and To date and time entered for the original query. It will not use the actual range entered in the original query. Also, it is important to remember that the time span between the From and To date and the time range used is relative to the date and time when the original query was run.

   Consider a query that is saved as a favorite and originally defined on 8/9/20xx to search reads between 8/02/20xx and 8/8/20xx (the prior week). If the Relative Date Range option is selected, the query is saved to always run against the prior week rather than those actual dates. If the Favorite option is invoked on 12/3/20xx, it will return results from 11/26/20xx through 12/2/20xx. It is important to note that the results will be relative to the actual time of the original query and when it is rerun. Suppose you run a query at 5 pm today to search for reads occurring between 9 am and 5 pm and save it as a favorite. When you run the query again tomorrow, it will search for reads that occurred eight hours **before** the current time, which may not necessarily fall between 9 am and 5 pm.
8. Click **OK** to complete. The query definition is now saved as a favorite and can be accessed at any time.

11.8.2 Activating a Favorite

1. Select the **Home** category in the Shortcut bar (if not already selected).
2. Click the **Favorites** shortcut.
3. A listing of all favorites is displayed in the Browse/Edit area.
4. Click the desired favorite. (The selected favorite will be highlighted in yellow.)
5. Click the **Go** button in the bottom area of the Browse/Edit area.
6. The query results will appear in the Browse/Edit area.

11.8.3 Deleting a Favorite

1. Select the **Home** category in the Shortcut bar (if not already selected).
2. Click the **Favorites** shortcut.
3. A listing of all favorites is displayed in the Browse/Edit area.
4. Click the desired favorite. The selected favorite will be highlighted in yellow.
5. Click the **Delete** button in the bottom area of the Browse/Edit area.
6. Press **Yes** to confirm deletion.

12 Reports

Several reports are included, automatically, with a new BOSS installation. These reports are available for use as soon as a BOSS Administrator assigns role permissions to the reports.

12.1 Running a System Report

1. Select the **Home** category on the Shortcut bar.
2. Click the **Reports** shortcut.
3. The Browse/Edit area will display a list of available reports. (Reports to which the user does not have permissions are not displayed.)
4. Click the desired report. The selected report is highlighted in yellow. Parameters for the report appear in the bottom of the Browse/Edit area.
5. Select **Date Range**. All reports call for From and To dates to define the time range for the report data. By default, the values in these fields define a report for the most recent two weeks. You can change these dates by typing different information into these fields, using the **Up/Down** arrow keys to the right of the field or by clicking the **Select** button to the right of the field and selecting a date on the calendar and then clicking the **Save** button.
6. Some reports also permit you to filter report results by user(s). For example, the pictures report, which reports pictures taken in LPCS, allows you to define one or more users to report on.
7. Once desired parameters are selected for the report, click the **Go** button. The report screen immediately displays, indicating that the server is generating the report until results are displayed.

12.2 Viewing and Printing Reports

The Report screen displays the date and time the report was generated and the title of the report in the heading area. When you place your mouse above a shortcut on the Report Shortcut bar, a label appears indicating what the shortcut button does. Note that some of the buttons on the Shortcut bar are not relevant to BOSS reports and are therefore disabled.

The Report Results Shortcut bar icons are as follows:



First Page – Return to the first page of the report.

Previous Page – Go to the previous page of the report.

Page Input – In this text box, type in a particular page number to bring up on screen.

Next Page – Go to the next page of the report.

Last Page – Go to the last page of the report.

Stop Rendering – This button can be used to cancel the report processing. This can be helpful if a large report was initiated, but is no longer desired.

Refresh – Refresh the report using the most current BOSS data.

Print – Print the report.

Print Layout – Toggle between available print layouts.

12.2 Viewing and Printing Reports *(continued)*

Page Setup – Choose among the options for standard page setup, such as page orientation, and paper size.

Save As – Excel/PDF/Word – Save the current results to a Microsoft Excel (.xls), an Adobe Portable Document Format (.pdf) or a Microsoft Word (.doc) document.

Width Zoom Setting – This drop-down list allows you to select a zoom view for the report results on the screen.

12.2.1 Viewing the Login Statistics Report

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut.
3. Click the **Logs** button at the bottom of the screen.



4. Click **Go** to view the Login Statistics Report.

   Begin Date – Select the start date for the report.

   End Date – Select the end date for the report.

   Selected Users – Select the users to include in the report. Click the **Select** button. Click the checkbox of the desired user. Click on the **Save** button.

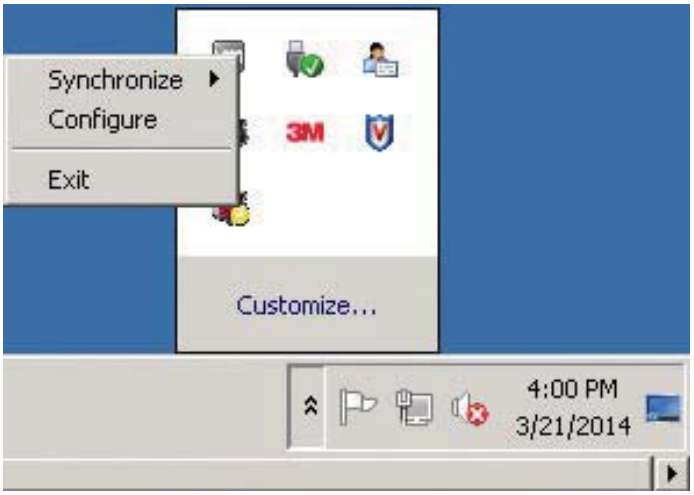
13 Client Tools

The Client Tools utility is used to transfer any necessary files needed for a shift from BOSS to an LPCS system that is being run in the Disk Sync mode. After the completion of a shift, Client Tools can then be used to transfer read data files captured during a shift into BOSS. The utility is configurable and processes files stored on a local, network, or USB flash drive. Like Smart Client, the Client Tools utility does not have to be run on the BOSS server; it can be configured to access the server via an IP Address.

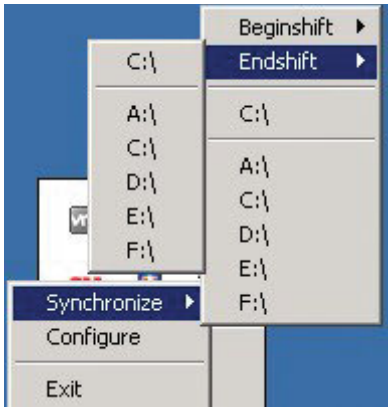
Client Tools does not have a customary interface. Once the utility is started, the Client Tools icon will appear in the Windows System Tray.

Before use, Client Tools must be configured, which is described in Appendix 17. Once the Client Tools has been configured, it can now be used to synchronize information between BOSS and LPCS:

1. To start, right-click on the **Client Tools** icon.



2. Select **Synchronize.** The next menu displayed is divided into three sections.
   a. The first section allows the user to select either **Create Begin Shift Files or Synchronize End Shift Files.** When either option is selected, the next menu is displayed. It is divided into two sections; it is the bottom two sections of the previous menu and functions the same way.
   b. The second section displays the path defined during configuration. This is a shortcut to perform Begin Shift and End Shift at the same time, storing the Begin Shift files in the defined location and processing the End Shift files at the defined location. If there are no End Shift files to process, this feature will be complete after the Begin Shift file is created. No error message will be displayed if the End Shift files are not found.
   c. The last section lists the drive letters currently on the workstation. If one is selected, Client Tools will perform a Begin Shift first and store the files at the root of the drive selected. Then Client Tools will check to see if there are End Shift files at that location. If found, the files will be processed. If not found, the synchronization process is complete. No error message will be displayed. This is an additional option if the configured drive is not currently available.



Note that once End Shift files have been processed, they are deleted.

14 Archiving Data

It is possible to archive reads that have accumulated in the BOSS database. Based on settings that are configurable in System Parameters, reads that meet the specified criteria are transferred from the main BOSS database to an archived BOSS database. *(See Section 15.3.2, List of BOSS System Parameters, for additional information on configuring this feature.)*

Once enabled, this process is handled by the BOSS server. There should be no noticeable difference to a user logged into a BOSS Smart Client when reviewing or reporting on stored reads. The only indication in the BOSS Smart Client that reads have been archived will be on the BOSS Home screen. The user will be able to see a calculable difference between the reads and hits counts compared to the total reads and total hits counts. The difference between the values will be the number of reads and hits stored in the archived database.

15 System Settings

15.1 Sessions

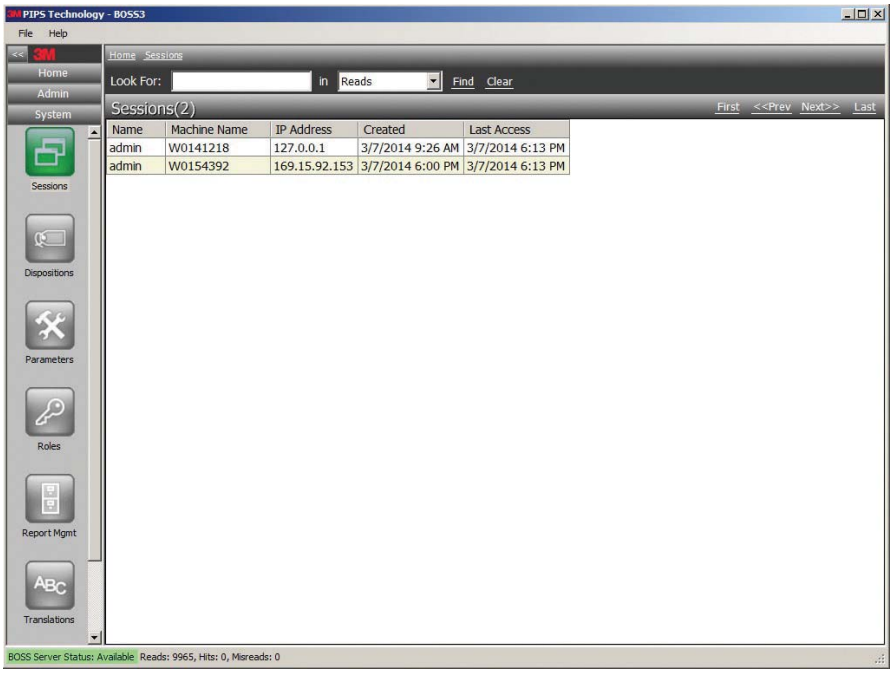
The Sessions screen allows for viewing the current list of logged-on BOSS users. Each login on each computer utilizes a concurrent license of the software. Since BOSS is licensed per concurrent active session, a BOSS Administrator may need to have a session disconnected in order to release a session license. A BOSS Administrator can force a session disconnect in the Sessions screen.

Note: BOSS allows a single "admin" login to access BOSS even if the number of concurrent sessions has been exhausted. *Please see Section 2.1, BOSS Administrator Login, for more information about the "admin" username.*

15.1.1 Viewing and Disconnecting Sessions

1. Select the **System** category on the Shortcut bar.
2. Click the **Sessions** shortcut. A list of current user sessions appears in the Browse/Edit area.
3. The heading in the Browse/Edit area indicates the total number of current sessions.
4. Click on a session to see details in the bottom half in the Browse/Edit area.
5. To disconnect, click the **Disconnect** button that appears in the detail area, and click **OK.**

Note: You cannot disconnect your own session in this manner. To disconnect your own session, simply log off the BOSS application.



15.1.2 Workstation Power Management and Sessions

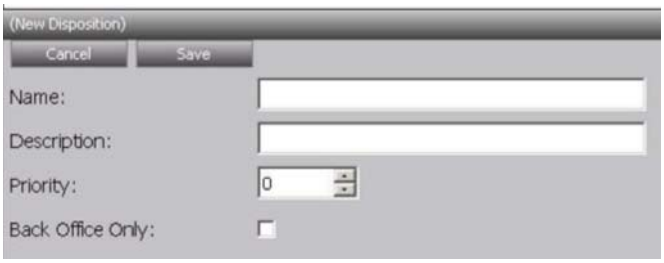
Using Windows Power Management to hibernate or suspend a workstation running the BOSS Smart Client will cause the session in BOSS to be terminated after five minutes. When the workstation is resumed from hibernation or a suspended state, the user will have to log in to BOSS again.

15.2 Dispositions

Dispositions are pre-defined classifications that can be assigned to hits. “Arrest Made,” “Vehicle Recovered,” “Surveillance Established” are examples of dispositions. A BOSS Administrator is able to define any number of dispositions for her system. Users can then use those dispositions to specify the action taken or the status of the hit. A new BOSS system will have a Default Disposition category that includes one disposition of “No Action.” Additional categories can be defined as needed.

15.2.1 Defining a New Disposition

1. Select the **System** category on the Shortcut bar.
2. Click the **Dispositions** shortcut. A list of all current dispositions appears in the top of the Browse/Edit area.
3. Click the **New** button in the bottom of the Browse/Edit area.
4. Enter a name for the disposition. If adding it to the default category, simply enter the name of the disposition. If adding it to a new category, the format of the name should be [Category : Disposition Name], i.e., **Auto :Vehicle Recovered.**
5. Enter a **Description** for the new disposition.
6. Specify a **Priority** for the disposition. (A lower number means a higher priority.)
7. Select the **Back Office Only** option if the disposition should not be available only in the Correct Reads screen in BOSS, and not exposed in LPCS.



15.2.2 Deleting a Disposition

1. Select the **System** category in the Shortcut bar (if not already selected).
2. Click the **Dispositions** shortcut.
3. A list of all dispositions is displayed in the Browse/Edit area.
4. Click the desired Disposition. The selected disposition will be highlighted in yellow.
5. Click the **Delete** button in the bottom area of the Browse/Edit area.
6. Press **Yes** to confirm deletion.

15.3 System Parameters

System Parameters allow for configuration parameters for a BOSS system. System parameters only need to be configured during initial system configuration and normally do not need to be modified again after that.

15.3.1 Editing System Parameters

1. Select **System** from the left Shortcut bar.
2. Click on the **Parameters** button in the Shortcut bar.
3. Click on the desired parameter in the right Browse/Edit window. The bottom pane of the Browse/Edit window will display the entry field for the selected parameter.
4. Modify the parameter value as desired and click the **Save** button.

15.3.2 List of BOSS System Parameters

arc_ActiveRetentionDays – This setting dictates how long reads will be maintained in the BOSS database. After reads have been stored for this time, they will be moved to the archived database, creating space for additional reads in the main database. The default setting is 730 days but can be varied based on the size and needs of the system.

arc_ArchiveDBRetentionDays – This setting dictates how many days to retain an archived database. After an archived database has been stored for this time it will be removed, creating space for additional archived databases. The default setting is 0 days, which indicates that the archived databases will never be removed, but the number of days can be modified based on the size and needs of the system.

arc_DatabaseLocation – This setting allows the user to specify where the archived databases should be saved. A blank entry will save them in the SQL default location.

arc_Enabled – To allow the BOSS server to archive aged reads and free up space, enable archiving by setting this to 1. When archiving is not desired, this setting should be 0.

arc_EndOfMonthCutOff – This setting forces a restriction on the size of the archived databases, so that nothing will be added after the end of each month. The default setting is disabled (0). To enable the setting, change the value to 1.

arc_MaxSize – This setting allows the Administrator to determine the number of reads that can be stored in the archived database. The default value is 1 million and can be varied based on the size and needs of the system. Once an archived database has reached this maximum number of records, a new archived reads database will be created.

audit_Justification_FileNumberRequired – When this setting is enabled (1), users performing read queries are required to enter a file number.This information will also be listed in the audit report. The default setting is disabled (0).

audit_Justification_NotesRequired – When this setting is enabled (1), users performing read queries are required to enter a justification note. This information will also be listed in the audit report. The default setting is disabled (0).

audit_JustificationEnabled – When this setting is enabled (1), users performing read queries are required to select a pre-defined justification. This information will also be listed in the audit report. The default setting is disabled (0).

data_CaptureUsageStatistics – When this setting is enabled (1), information sent from a LPCS device that has been modified due to Privacy settings will still be utilized to generate usage statistic reports. The default setting is disabled (0).

hls_HotListDeltas – When this setting is enabled (1), updated hotlists will be deployed in full. Changing the setting to disabled (0) will cause only the changes made in the updated hotlists to be deployed.

15.3.2 List of BOSS System Parameters *(continued)*

Proxy_uri/proxy_username /proxy_password/proxy_domain – These settings are only necessary if there is a proxy server involved that requires authentication for connection. Enter a valid Uniform Resource Identifier (URI), username, password, and domain in the associated fields to allow communication through the proxy server. Consult the network Administrator for proxy authentication information

purge_Minutes – This setting is the time, in minutes, between each session of purging or archiving. The default value is 15 minutes and is configurable to any value of 1 minute or greater.

purge_ReadCount – This setting is the number of records to be processed by the purging or archiving process per session. It can be any value, but setting it according to system limitations is recommended because the process can be resource intensive if set too high.

readQuery_fromDate – This setting allows the user to adjust the default From date on the Reads Query screen. Any value can be entered and it is used to decrement from today. Example – a value of 7 would result in a From date seven days earlier than today.

readQuery_toDate – This setting allows the user to adjust the default To date on the Reads Query screen. Any value can be entered and it is used to incremented from today. Example – a value of 7 would result in a To date seven days later than today.

rq_ReaperHours – This setting manages how long to retain a temporary database table created when running certain read queries. This allows the user to continue to review the results of those queries for a longer time. The default is a minimum of 48 hours, and there is no maximum value.

smtp_SenderName – In order for the BOSS server to send alerts to email addresses, the SMTP settings must be configured correctly. The SMTP sender field should contain the username that will appear in the From field on an email generated by the BOSS system.

smtp_Server – The name or IP address of the SMTP server should be entered here. The name or address used here must be one by which the SMTP server can be reached from the BOSS server. This field must be populated correctly in order for the BOSS system to send any alerts to email addresses.

smtp_UserName/smtp_password – The SMTP username and password fields should contain a valid SMTP username and associated password for sending alerts through the SMTP (email) server. Normally, a BOSS Administrator coordinates with his SMTP Administrator to create a special SMTP user that will be used exclusively for BOSS alerts.

smtp_SSL – If Secure Sockets Layer (SSL) is used on your SMTP server, the value of this field should be set to 1. If you do not use SSL, this field should be set to 0.

smtp_SubjectTemplate /smtp_AlertTemplate – These fields allow a BOSS Administrator to customize the verbiage in an alert email subject line and message body using any combination of static text and field variables from the hit that generated the alert. Each field (from the hit) is enclosed in brackets.

smtp_SubjectTemplate – This field sets the subject line of alert emails generated by BOSS.

smtp_AlertTemplate – This field determines the text in the body of the alert email.

For example, the following entry in the smtp_SubjectTemplate field incorporates both static text and a BOSS field variable as well: **BOSS alert FROM [SRC]**

The static text “BOSS alert FROM” will always be constant in each SMTP alert. However, the value of [SRC] will vary depending upon the source device where the hit originated. If the hit originated from a source device named “Camera2,” for instance, the complete subject would read: “BOSS alert FROM Camera2”.

The following tokens can be used in the templates, and for each individual alert they will be replaced with the actual value from the hit record:

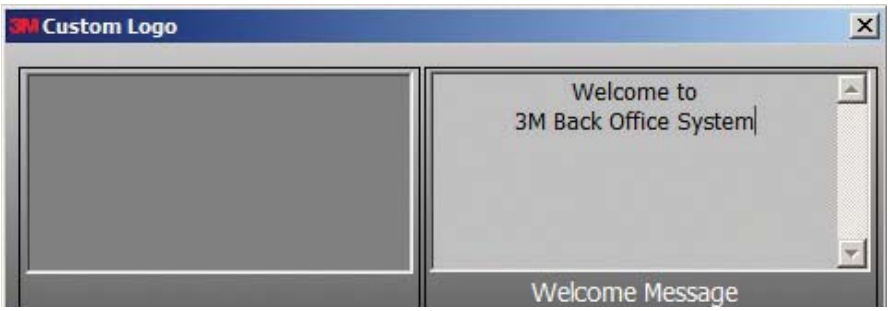


TOKEN	DESCRIPTION
[LPN]	license plate
[STE]	site
[SRC]	device
[LOC]	location
[LAT]	latitude
[LON]	longitude
[HOT]	hotlist name
[FD1]	field1
[FD2]	field2
[FD3]	field3
[FD4]	field4
[FD5]	field5
[PNC]	PNCID/DL
[INF]	information
^	new line

15.3.3 Branding

BOSS allows the BOSS Administrator to upload a logo image and a welcome message that is displayed to BOSS users on the Home screen. To define the image and message:

1. Select **System** from the left Shortcut bar.
2. Click on the **Parameters** button in the Shortcut bar.
3. Click on **Branding.**
4. If needed, click **Default** to remove current custom settings.
5. Pick the desired logo image using the **Browse…** button.
6. Type in a message in the Welcome Message box.



Browse – Select an image file (JPEG, GIF, BMP) to be displayed on the home screen. The largest recommended image size is 120 by 380 pixels.

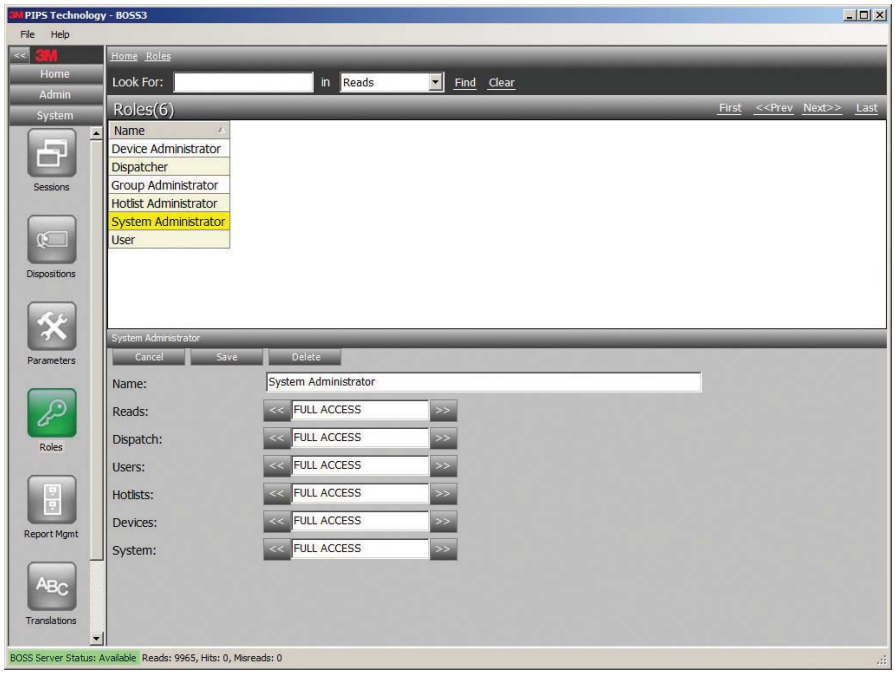
Default – Remove the custom logos and texts.

Welcome Message – A custom welcome message can be typed in here.

7. Click **OK** to save changes, or Cancel to discard changes.

15.4 Roles

In addition to the default roles that are automatically created by BOSS, the Administrator can create and configure custom roles as needed. *See Section 4.2, Permissions, for more information.*



15.4.1 Adding New Roles

1. Select the **System** category on the Shortcut bar.
2. Click the **Roles** shortcut. The Browse/Edit area will display a list of existing roles.
3. Click on the **New** button. The New Role entry window will be displayed in the bottom of the window.
4. Enter the name of the new role and assign the desired permissions.
5. Click the **Save** button.

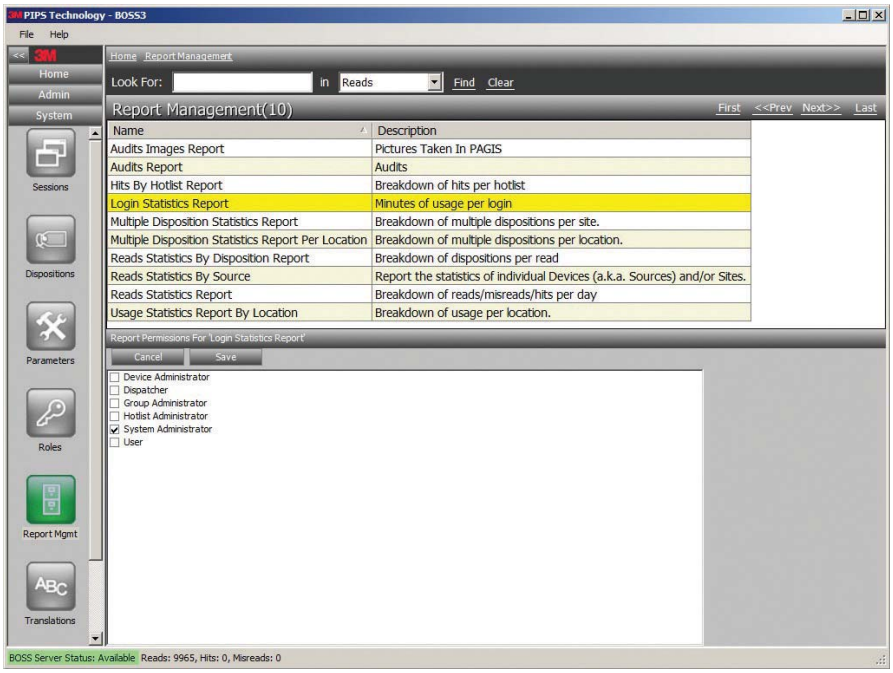
15.4.2 Deleting Roles

1. Select the **System** category on the Shortcut bar.
2. Click the **Roles** shortcut. The Browse/Edit area will display a list of existing roles.
3. Click on an existing role and the edit window will be displayed in the bottom of the window.
4. Click the **Delete** button. Click **Yes** when prompted to complete the operation.

15.5 Report Management

15.5.1 Assigning Permissions to Access Reports

1. Select the **System** category on the shortcut bar.
2. Click the **Reports Mgmt** shortcut. The Browse/Edit area will display a list of available reports.
3. Select a report by clicking the name in the list. The selected report will be highlighted in yellow.
4. Current report permissions for the type of report chosen display in the bottom of the Browse/Edit area. Each BOSS role is listed along with a checkbox. Click a role in the list to select. Click a second time to change an unchecked box to a checked box.
5. After selecting the desired permissions for the report, click the **Save** button.

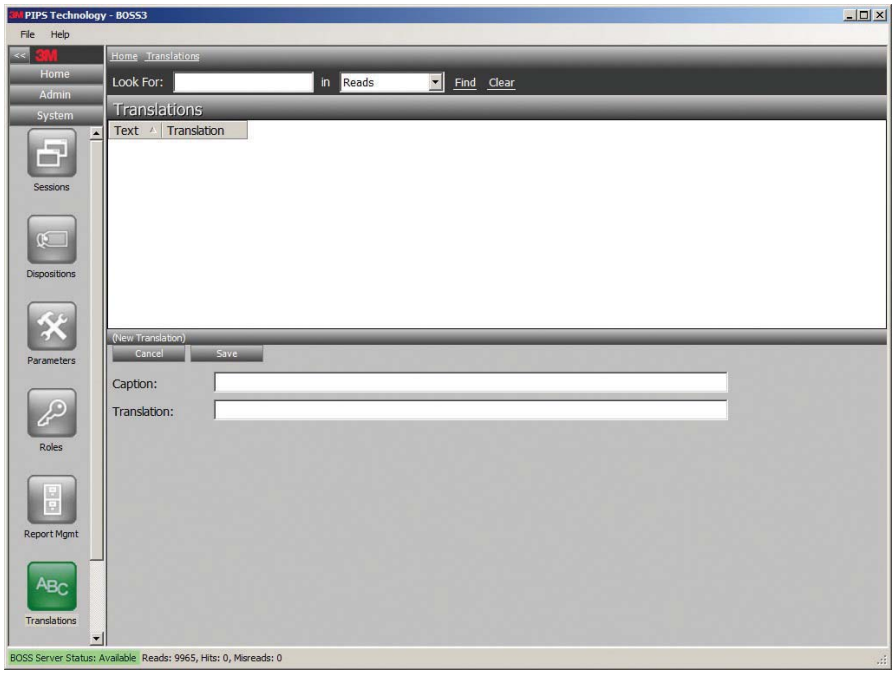


15.6 Translations

Across various organizations and agencies, terminology related to BOSS can differ significantly. For this reason, a new function added in the BOSS version 3 series gives customers flexibility in naming conventions used in the application. The Translations function provides for changing wording on BOSS screens, which allows a customer to tailor screen labeling to correspond to their own vernacular. Text items in the translations editor correspond to labels on BOSS screens. Authorized users can change these text items as necessary.

Note: This feature is not intended as a replacement for language-specific versions of BOSS. *For international versions of BOSS, please contact 3M Technical Support.*

15.6.1 Entering a New Translation



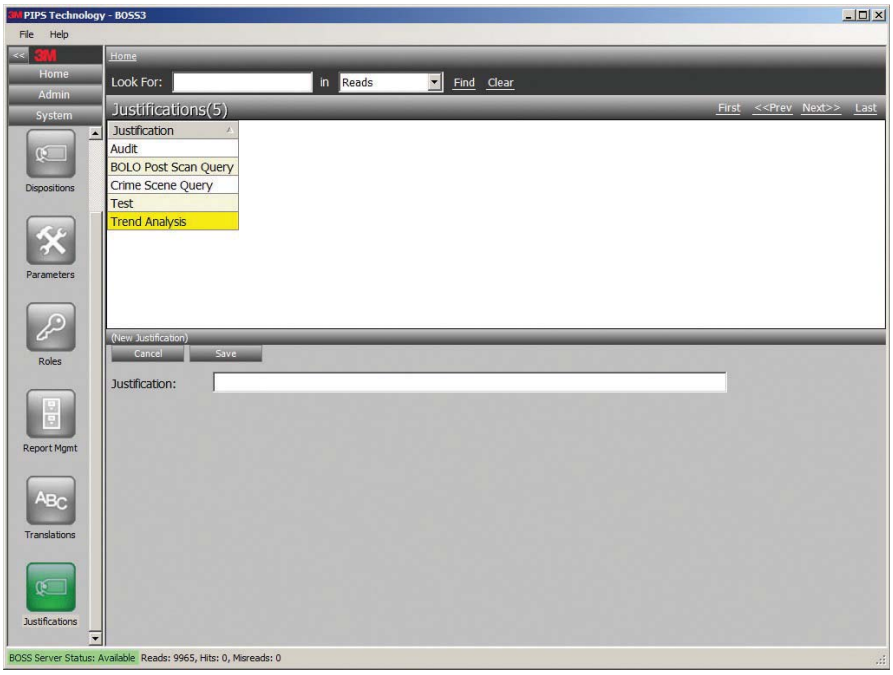
1. Select the **System** category on the Shortcut bar.
2. Click the **Translations** shortcut. A list of all current translations appears in the top of the Browse/Edit area.
3. Click the **New** button and the new Translations Entry screen appears in the bottom area.
4. Enter an existing label from the BOSS application in the Caption field, using the exact case and spelling that normally appears on the screen.
5. Enter the desired replacement text in the Translation field.
6. Click the **Save** button to complete the operation.

Note: The user must log off and on again for translation to take effect in the current session.

For Example: A customer preferring to see a label of “Plate” where the software normally uses the term “LPN” would use the translations feature to create the replacement for their installation. The translation Entry Caption field would contain “LPN,” while the Translation field would contain the replacement term “Plate.”

15.7 Justifications

To ensure that sensitive information is being kept secure, systems can be configured to require that users who are performing queries on reads have a valid reason for doing so. Enabling the audit_JustificationEnabled parameter requires users to justify their reason for querying reads. There are five justifications created by default: Audit, BOLO Post Scan Query, Crime Scene Query, Test and Trend Analysis. These queries will also be documented in audit reports.



15.7.1 Entering a New Justification

1. Select the **System** category on the Shortcut bar.
2. Click the **Justifications** shortcut. A list of all existing justifications appears in the top of the Browse/Edit area.
3. Click on the **New** button. The Justifications Entry screen appears in the bottom area.
4. Enter a justification. There is no validation on the entry for this field.
5. Click the **Save** button to complete the operation.

15.7.2 Deleting Justifications

1. Select the **System** category on the Shortcut bar.
2. Click the **Justifications** shortcut. A list of all existing justifications appears in the top of the Browse/Edit area.
3. Click on the justification to be deleted. The Justifications Edit screen appears in the bottom area.
4. Click the **Delete** button. Click on **Yes** when prompted to complete the operation.

16 Appendix: System Requirements

16.1 *Minimum* System Requirements

Please note that the minimum requirements are the *least* resources needed to run the software. We fully expect 3M Back Office System Software to run in these environments. However, the user may experience periods of slowness. There may also be other environmental factors that could impact the application's performance such as networks, the utilization of resources by other processes, etc.

16.1.1 Smart Client Minimum System Requirements

If the Smart Client is installed on a workstation, the minimum system resources needed for installing and running the 3M BOSS 3.2 or above Smart Client are:

- Pentium-compatible PC at 1.0 GHz
- Windows Vista, Windows 7, or Windows 8
- 1 GB of RAM
- 32-bit SVGA display at 1024 x 768 pixels
- 1 GB of hard drive space
- Keyboard and mouse

16.1.2 BOSS Server Minimum System Requirements

If 3M BOSS 3.2 or above is being run on a dedicated system, the minimum system resources needed for installing and running the BOSS Server are:

- Intel Xeon Quad Core CPU at 2.0 GHz
- Windows Vista, Windows 7, or Windows 8, 64-bit mode
- 8 GB of RAM
- 1 GB of hard drive space
- Microsoft SQL Server 2008 Express Edition, on a separate machine

If 3M BOSS 3.2 or above is being run on the same system as the SQL Server, the minimum system resources needed for installing and running both are:

- Intel Xeon Quad Core CPU at 2.0 GHz
- Windows Vista, Windows 7, or Windows 8, 64-bit mode
- 16 GB of RAM
- 1 GB/20,000 reads of hard drive space
- Microsoft SQL Server 2008 Express Edition, with memory usage constrained

16.1.3 SQL Server Minimum System Requirements

If SQL Server is being run on a dedicated system, the minimum system resources needed for installing and running the SQL Server are:

- Intel Xeon Quad Core CPU at 2.0 GHz
- Windows Vista, Windows 7, or Windows 8, 64-bit mode
- 16 GB of RAM
- 1 GB/20,000 reads of hard drive space
- Microsoft SQL Server 2008 Express Edition

16.1.4 Client Tools Minimum System Requirements

The minimum system resources needed for installing and running the 3M BOSS 3.2 series Client Tools are:

- Pentium-compatible PC at 1.0 GHz
- Windows Vista, Windows 7, or Windows 8
- 1 GB of RAM
- 32-bit SVGA display at 1024 x 768 pixels
- 1 GB of hard drive space
- Keyboard and mouse

16.2 Recommended System Requirements

16.2.1 Smart Client Recommended System Requirements

The recommended system requirements for installing and running the 3M BOSS 3.2 series Smart Client are:

- Pentium-compatible PC at 1.0 GHz
- Windows Vista, Windows 7, or Windows 8
- 2 GB of RAM
- 32-bit SVGA display at 1024 x 768 pixels
- 1 GB of hard drive space
- Keyboard and mouse

16.2.2 BOSS Server Recommended System Requirements

If the 3M BOSS 3.2 or above service is running in a dedicated environment, the recommended system requirements for installing and running the 3M BOSS Server are:

- Intel Xeon quad-core CPU at 2.0 GHz or faster
- Windows Server 2008 Standard Edition in 64-bit mode
- 16 GB of RAM
- SCSI or SAS hard drives at 10,000 RPM

- 1 GB of hard drive space
- Microsoft SQL Server 2008 R2 Standard Edition, on a separate system

If the 3M BOSS 3.2 or above is being run on the same system as the SQL Server, the recommended system requirements for installing and running both are:

- Intel Xeon quad-core CPU at 2.0 GHz or faster
- Windows Server 2008 Standard Edition in 64-bit mode
- 32 GB of RAM
- SCSI or SAS hard drives at 10,000 RPM
- 1 GB/20,000 reads of hard drive space
- Microsoft SQL Server 2008 R2 Standard Edition, with SQL memory usage constrained

16.2.3 SQL Server Recommended System Requirements

If the SQL Server is running on a dedicated system, the recommended system requirements for installing and running it are:

- Intel Xeon quad-core CPU at 2.0 GHz or faster
- Windows Server 2008 Standard Edition in 64-bit mode
- 32 GB of RAM
- SCSI or SAS hard drives at 10,000 RPM
- 1 GB/20,000 reads of hard drive space
- Microsoft SQL Server 2008 R2 Standard Edition

16.2.4 Client Tools Recommended System Requirements

The minimum recommended system requirements for installing and running the 3M BOSS series Client Tools are:

- Pentium-compatible PC at 1.0 GHz
- Windows Vista, Windows 7, or Windows 8
- 2 GB of RAM
- 32-bit SVGA display at 1024 x 768 pixels
- 1 GB of hard drive space
- Keyboard and mouse

17 Appendix: Installation and Configuration

This section is intended for authorized personnel in installation and configuration of a BOSS system. The information in this guide is organized sequentially, in the order that steps would be performed when initially setting up a new BOSS system, with the first section describing the software installation process, and the subsequent sections describing configuration options for a BOSS system.

Upon initial installation of a new BOSS system, the BOSS server application must be configured using the BOSS Controller application. BOSS Administrators may also find the need to modify configuration settings after the system has already been in use. Therefore, the configuration section can be used as an ongoing reference for authorized personnel responsible for maintaining the system.

IMPORTANT NOTE: It is critical that **only an IT Administrator or other knowledgeable personnel** attempt configuration modifications to a BOSS system. Incorrect configuration settings can cause serious issues with operation and/or adversely affect data integrity. When in doubt, you should consult 3M Technical Support before making system configuration changes.

17.1 Installing the BOSS Server Application Files

17.1.1 Running the Installer

This guide assumes that the Microsoft SQL Server 2008 instance for BOSS has already been installed and is available. If the SQL Server is not available, *stop now and continue installation after the SQL Server has been installed.* To install the Microsoft SQL Server, please follow the instructions provided by Microsoft.

Note: 1. It is not recommended that the installation be performed over a remote desktop connection.

2. It is recommended that antivirus utilities be disabled during the install.

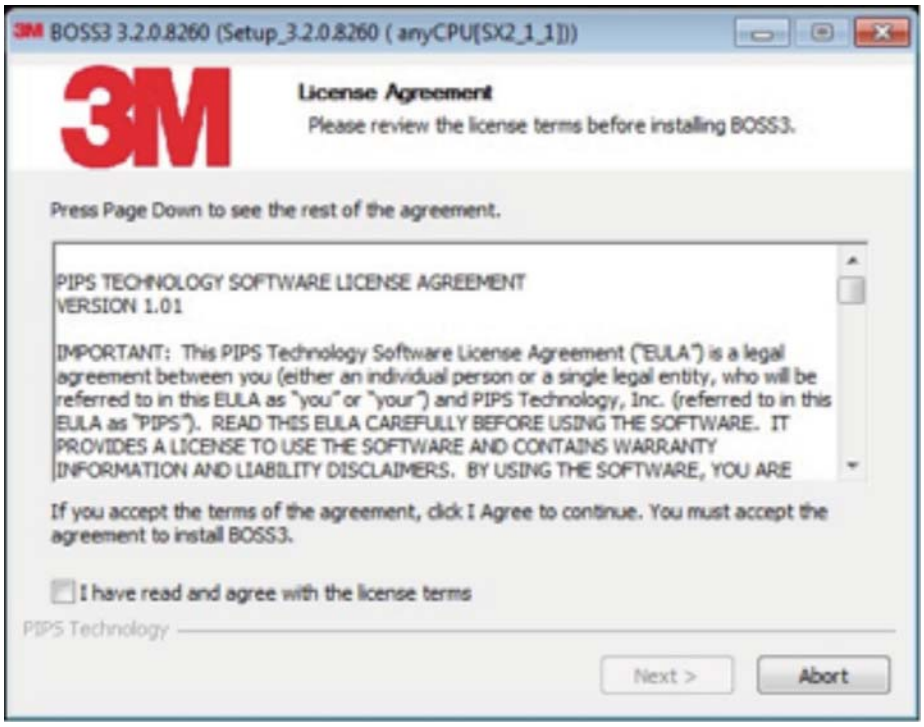
To commence the installation:

1. Select the link supplied by 3M to the BOSS 3.2 installation application.
2. Run the BOSS 3.2 Setup executable.

Note: Right-click on the installer icon and select **Run As Administrator**.

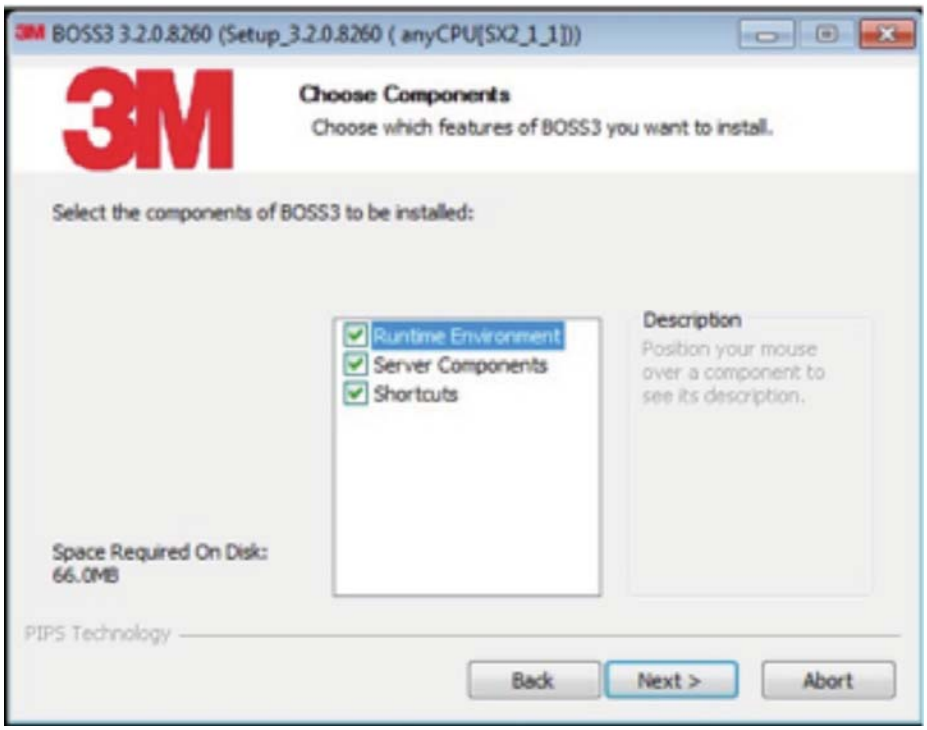
17.1.2 3M License Agreement

1. Click the license agreement checkbox to acknowledge agreement with the license terms.
2. Click **Next** to continue.



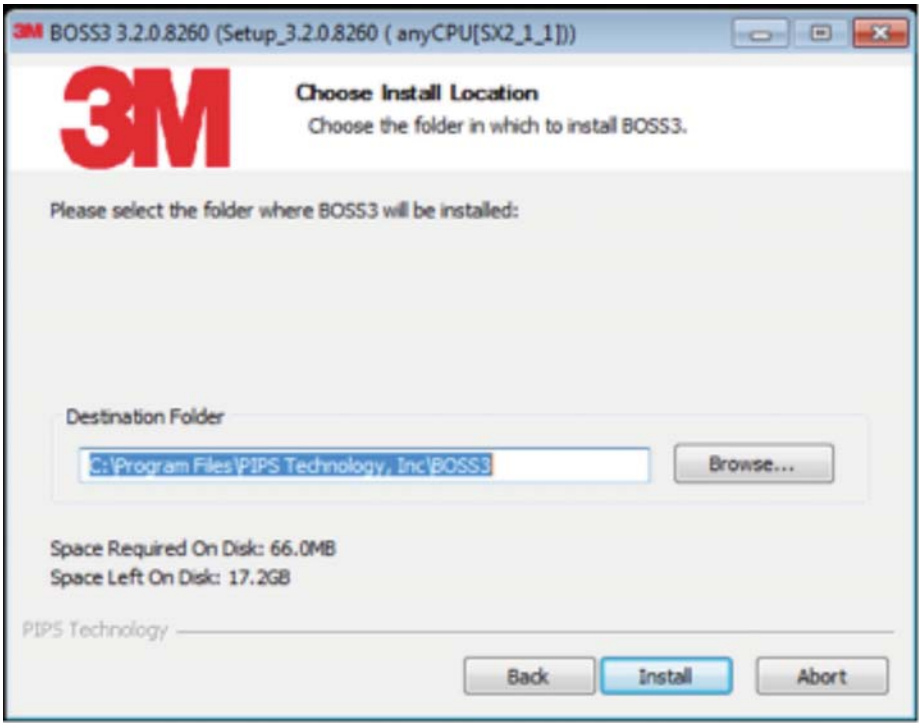
17.1.3 Selecting the Installed Components

1. Check the box for each component you wish to install for BOSS 3.2.
    - Runtime Environment (required)
    - Server Components (required)
    - Shortcuts (optional)
2. Click **Next** to continue.

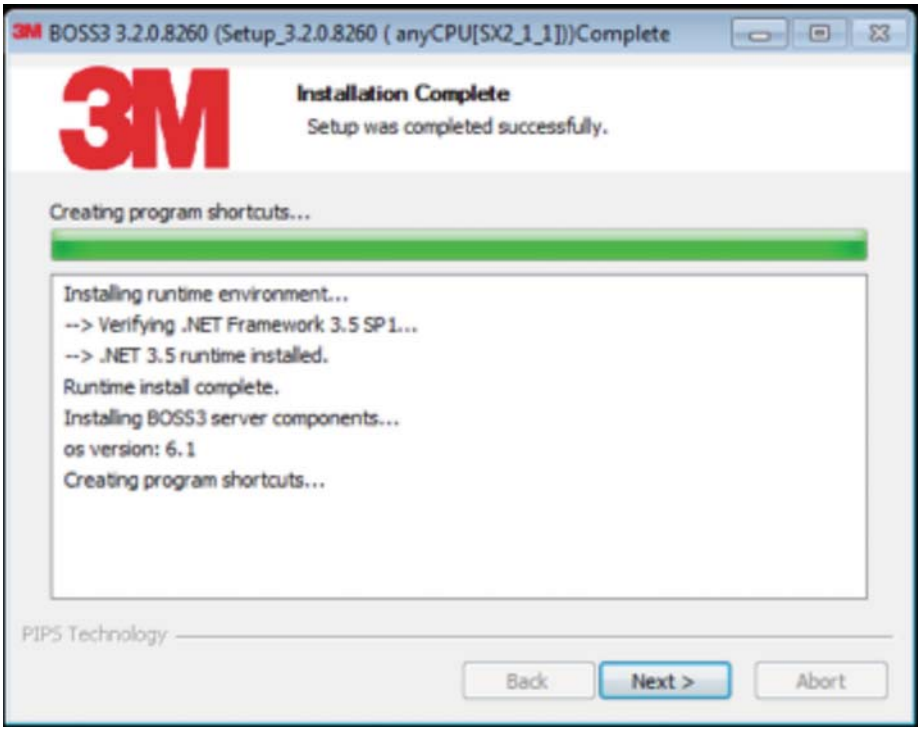


17.1.4 Selecting the Installation Folder

1. Select the location to install BOSS 3.2 by browsing your drive or typing a location.

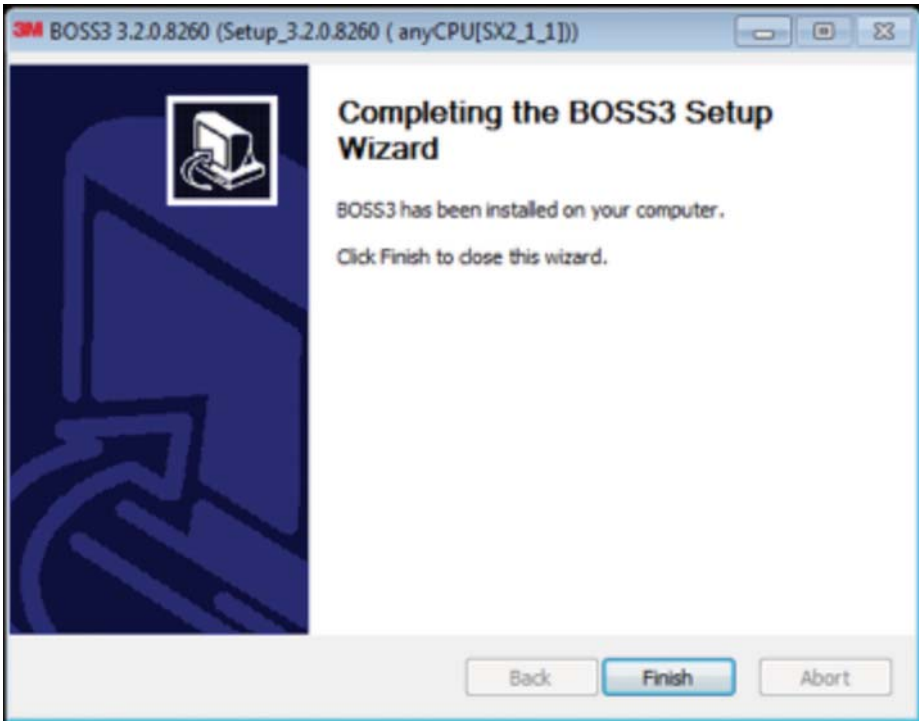


2. Click **Install.** The installation will then commence.



17.1.4 Selecting the Installation Folder *(continued)*

3. When the Installation Complete message is displayed, click **Finish** to proceed to the Licensing Wizard.

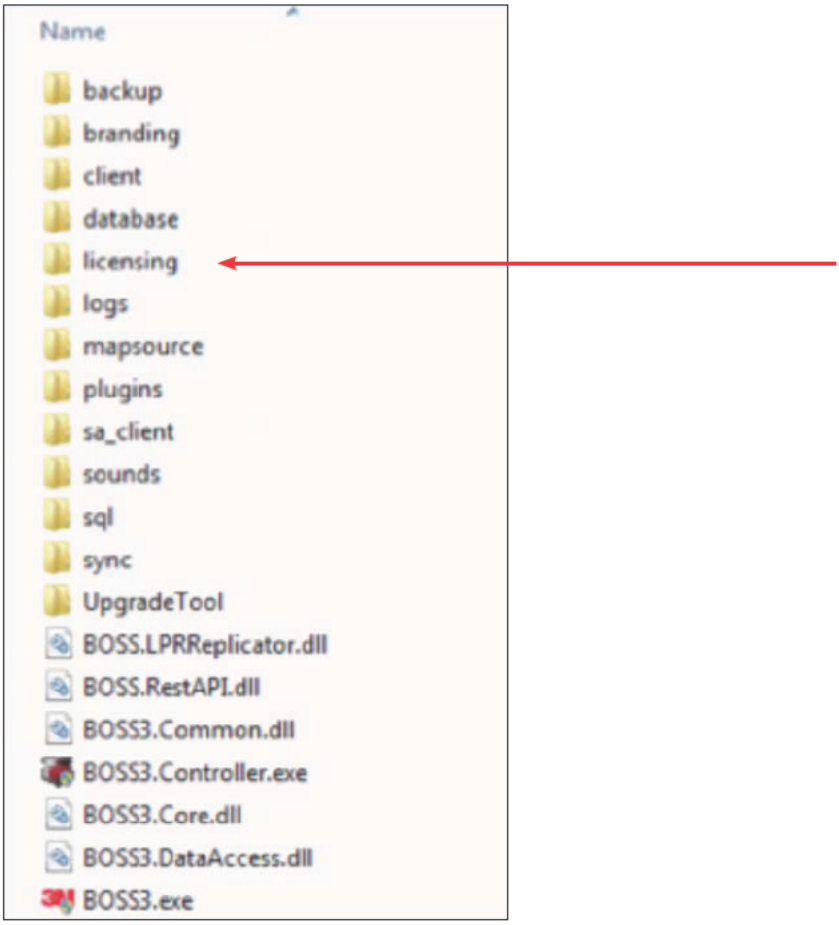


17.2 BOSS Version 3.2 and Above License Key Management

17.2.1 Activating the License Key

Following a new installation, a valid BOSS 3.2 license key must be entered. There are three options available discussed in the sections below that can be used to activate the license.

1. Navigate to the licensing folder in the BOSS 3.2 installation folder.



2. Start Microsoft License Manager (**Microsoft.Licensing.LicAdmin.exe**). This must be run as an Administrator.
3. In the License Manager User interface, select **File → Activation Wizard** to install the new license.
4. When the Activation Wizard dialog opens select one of the following:
    a. I want to activate the software over the Internet. *See Section 17.2.1.1.*

    or

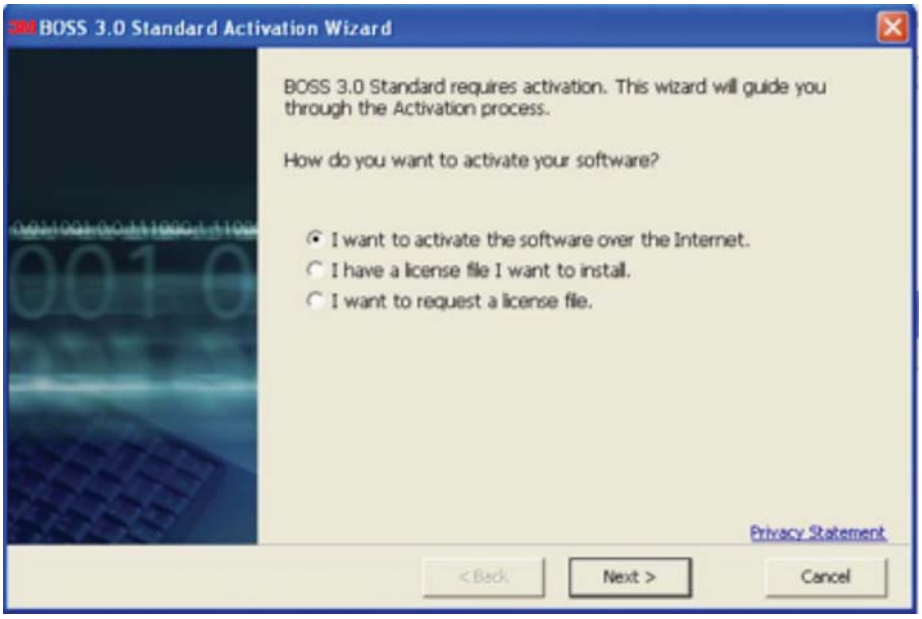
    b. I have a license file I want to install. *See Section 17.2.1.2.*

    or

    c. I want to request a license file. *See Section 17.2.1.3.*

17.2.1.1 Activating the License Key over the Internet

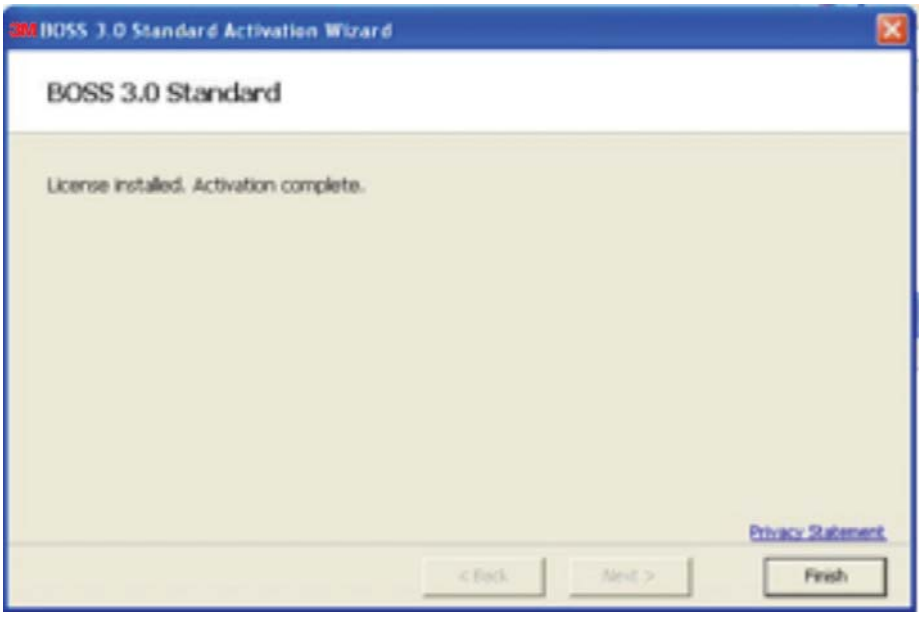
1. Check **I want to activate the software over the Internet**.
2. Click **Next** to continue.



3. Enter the activation key provided by 3M and click **Next.**



4. The license key will be activated over the Internet. The following screen will display. Click **Finish** to continue.



17.2.1.2 Activating the Software with a License File

1. Check **I have a license file I want to install.**
2. Click **Next** to continue.
3. Navigate to the location of the license file and select it.
4. Click **Next** to continue.
5. When the activation is completed click **Finish.**

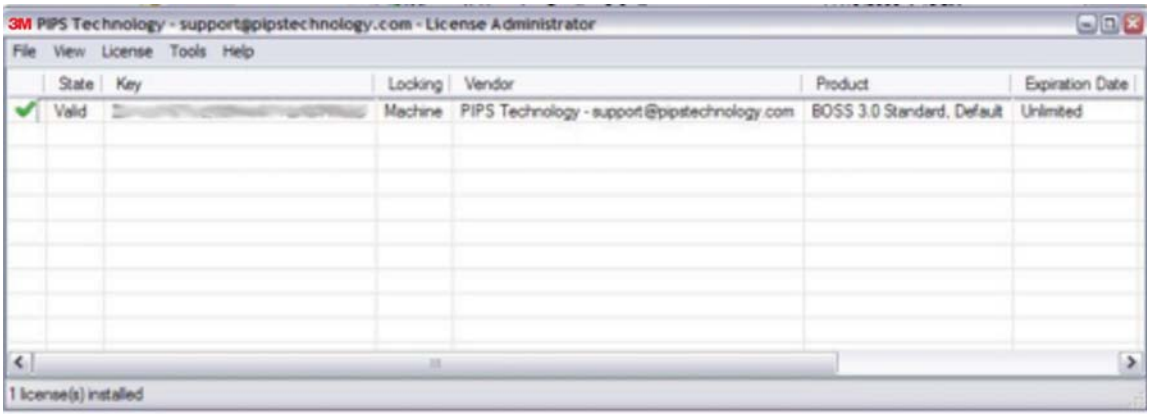
17.2.1.3 Request a License File to Activate the License

1. Click **I want to request a license file.** Press **Next.**
2. Enter the license key you received previously. Press **Next.**
3. In the screen that displays, copy the text block highlighted (starts with "—BEGIN Request") to the clipboard and paste it into an email. Send the email to 3M Technical Support (alprsupportus@mmm.com).
4. Close the Activation Wizard by clicking the **Finish** button.
5. You will be sent an activation file via email. Extract the license file (*.bin) and copy it to a folder on the computer where BOSS is installed. *Return to Section 17.2.2 and follow the steps to activate the license.*

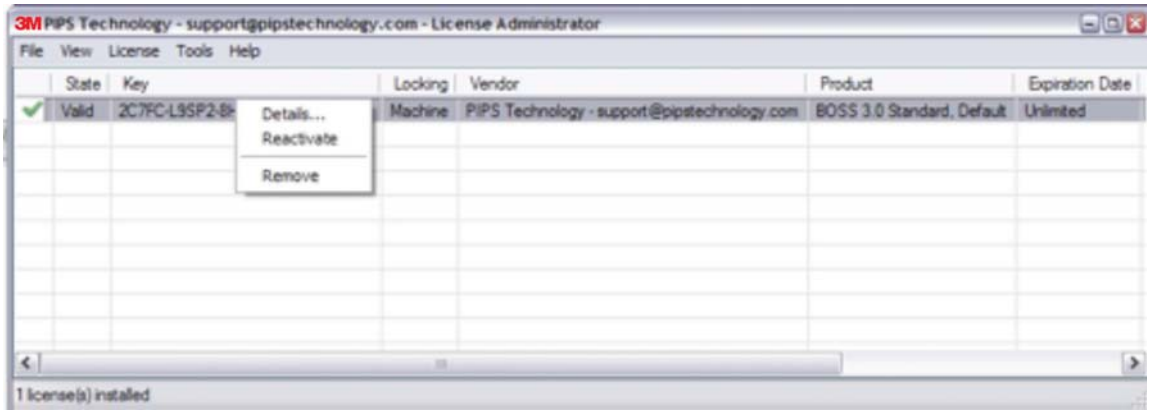
17.2.2 Updating a License Key

If the BOSS license key becomes invalid, or if the license is upgraded, follow these steps to reactivate a BOSS license key:

1. Start Windows Explorer on the BOSS server.
2. Navigate to the folder where the BOSS server application is installed (by default C:\Program Files\PIPS Technology, Inc\BOSS3).
3. Locate the licensing folder as described in Section 17.2.1.
4. Open the folder and right click on the application **Microsoft.Licensing.LicAdmin.exe.** Select to run as the Administrator. You will see the following screen:



5. Select the license key. Right-click, and from the context menu, select **Reactivate.**



6. Click **Next.**
7. When the Installation Complete message is displayed, click **Finish.**

17.3 Map Display Options with BOSS

BOSS version 3.2 and above can display collected plate read information plotted on a map. There are two different mechanisms for displaying maps within the BOSS Smart Client application.

17.3.1 U.S. Census Bureau TIGER Maps

BOSS supports downloading U.S. Census Bureau Topologically Integrated Geographic Encoding and Referencing (TIGER) maps data into BOSS. This data is available free of charge within BOSS. TIGER maps will work without an Internet connection once the data has been downloaded.

TIGER maps cover the United States and its territories. Because these are very large data files, geographical coverage of a download should be limited to a few counties. Also, because of the limited nature of Census information, address search with TIGER maps is approximate (per census block). If more coverage or more accuracy is required, other mapping options should be considered. Satellite imagery is not available with TIGER maps.

17.3.2 Advanced Mapping with Microsoft Bing Maps

3M provides an option to purchase an “Advanced Mapping” feature with BOSS. This option enables integration of Microsoft Bing® Maps, an Internet-based service that BOSS can use to display maps in the Smart Client application.

Note: In order to use Advanced Mapping, the BOSS server and each Smart Client workstation will need an unimpeded Internet connection to Microsoft.com (no proxy servers). Bing Maps supports accurate address search and satellite imagery.

For more information about Bing Maps, please go to: http://www.bing.com/maps

17.4 Configuring the BOSS Server Application

After the BOSS version 3.2 or above installation is completed, the application must be configured using the BOSS Controller program. The following sections explain how to use this program as well as the configuration settings that are available.

17.4.1 The BOSS Controller Application

17.4.1.1 Starting the Boss Controller

BOSS Controller (BOSS3.Controller.exe) is the application used to configure and control the BOSS service. The BOSS Controller is installed on the server computer along with the server application. After the installation is complete the Controller program will start automatically. If this is a new installation the license will need to be activated first. Choose to configure BOSS at a later time by clicking on **Cancel.**

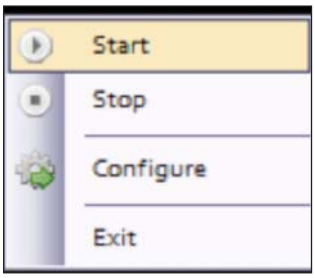
The shortcut to the BOSS Controller program can be found on the desktop or in the All Programs → PIPS Technology → BOSS3 menu. Right-click on the Controller icon and select **Run As Administrator.** When the BOSS Controller program is started an icon for the application will appear in the Windows System Tray at the lower right corner of the desktop.

17.4.1.2 Status Colors

The icon for the Controller program includes a “traffic light” that uses a color indicator to show the status of the BOSS service application. When the BOSS service application is running, the indicator is green. When the BOSS service application is not running, the indicator is red. Yellow color indicates that the application is changing state (starting or stopping).

17.4.1.3 Right-Click Menu

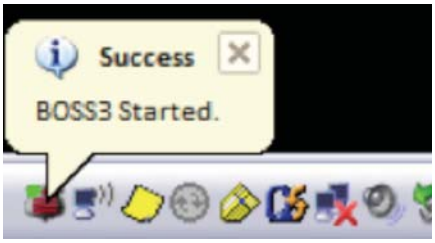
When you right-click the BOSS Controller System Tray icon, a pop-up menu will appear:



Start	Start the BOSS service.
Stop	Stop the BOSS service.
Configure	Present the BOSS Configuration Wizard.
Exit	Close the BOSS Controller application. (**Note:** This closes the BOSS Controller program, but does not stop the BOSS Service.)

17.4.1.4 Starting the BOSS Service

When the **Start** action is selected, and the service starts successfully, a Success message will be displayed:



The traffic light in the BOSS Controller icon will turn green to indicate the status.

17.4.1.5 Stopping the BOSS Service

When the **Stop** action is selected, and the service stops successfully, another Success message will be displayed, and the traffic light changes to red:



17.4.2 BOSS Configuration

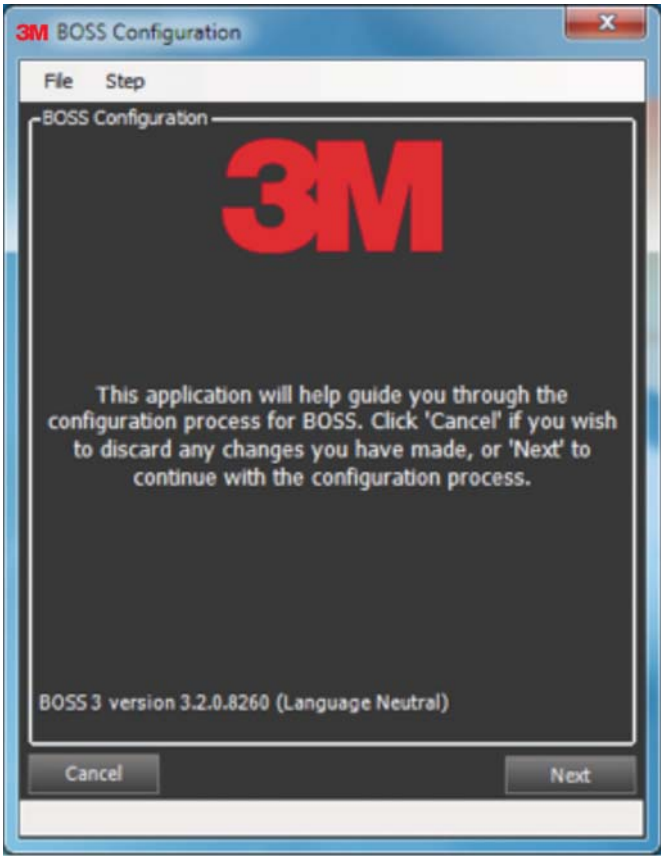
17.4.2.1 Activating the Configuration Wizard

If this is a new installation of the BOSS application, the Configuration Wizard will automatically display after the installation of the files is complete.

If the BOSS Configuration Wizard is displayed, go to Section 19.4.2.2, BOSS Configuration Wizard. If the Configuration Wizard is not displayed:

1. Right-click the **Controller System Tray** icon.
2. Select the **Configure** option. The Configuration Wizard options are explained in the following sections.

17.4.2.2 BOSS Configuration Wizard



Step through all configuration screens in the BOSS Configuration Wizard by simply clicking the **Next** button on this first screen. Click **Next** on each subsequent screen after entering in the desired settings. **Note:** This step-by-step process is recommended when you are configuring the system for the first time.

OR

Click the **Step** menu option to access the configuration menu and proceed to the step choice.

For each configuration step (described in Sections 17.4.2.3 – 17.4.2.9), clicking **Next** will take you to the next configuration screen, clicking **Previous** will take you to the previous one, and clicking **Cancel** will clear any changes you have made on the current screen.

17.4.2.3 SQL Server Configuration

SQL Server configuration is required for a new BOSS system, in order to specify the location and necessary authentication information for the SQL database.



SQL Server – Select the SQL Server 2008 instance for BOSS. Press **List** to choose from a list of available SQL Servers. The SQL Server Browser service must be running at this point. You may also type in the server IP address or host name. Enter a dot "." to use a local SQL Server that is running on the same machine as the BOSS service.

Use Windows Integrated Security – If checked, BOSS will use Windows Integrated Security to access the SQL Server database.

SQL Server Login and SQL Server Password – If Windows Integrated Security is not selected, enter the SQL Server username and password provided for BOSS to use to access the database.

Test – The **Test** button can be used to test the SQL Server settings currently in place. The **Test** button initiates a connection. A message box will appear to indicate whether the test connection fails or succeeds.

BOSS requires approximately 1 GB of hard drive space per 20,000 reads. In order to improve performance, the BOSS database can be divided among multiple locations as follows:

Primary Database Folder – The drive and folder where the BOSS primary database will reside

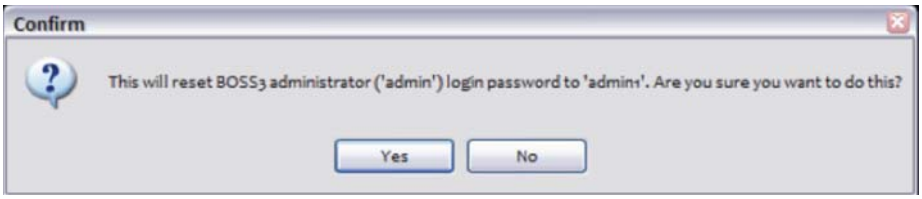
Images Database Folder – The drive and folder where the BOSS will store images

Reads Index Folder – The drive and folder where BOSS will store database indices for stored plate reads

Transaction Log Folder – The drive and folder where BOSS will store the database transaction log file

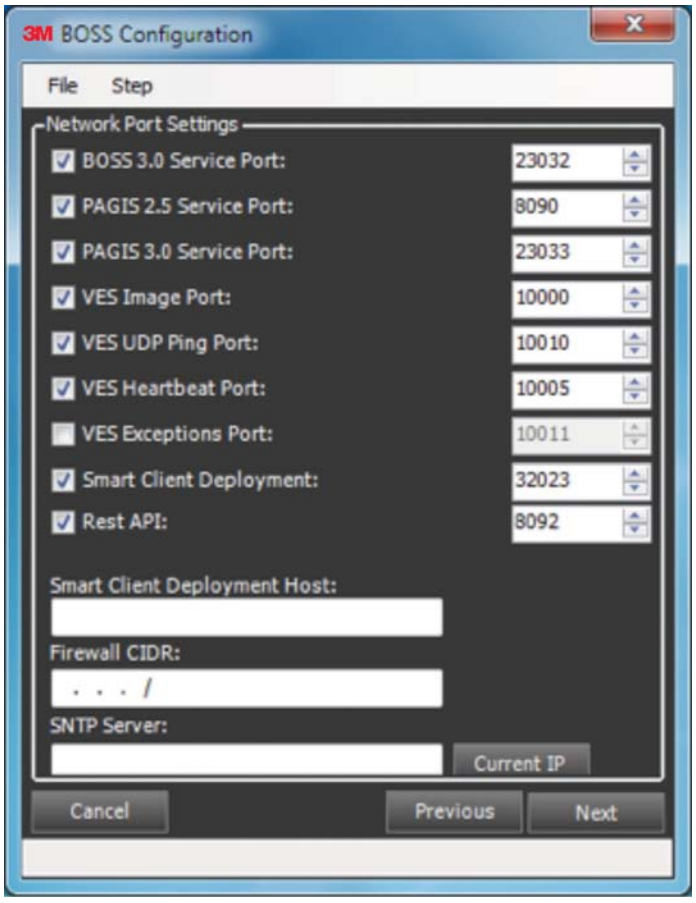
17.4.2.4 Resetting the Administrator Password

If you have forgotten the BOSS administrator (admin) password, you can press the **Reset 'admin' password** button to reset the password to "admin1."



Pressing **Yes** will immediately reset the password.

17.4.2.5 Network Port Settings



BOSS uses a number of TCP/IP and UDP network ports for communication between server and client applications and server and license plate reading devices.

17.4.2.5 Network Port Settings *(continued)*

FIELD	DESCRIPTION	DEFAULT PORT
BOSS 3.0 Service Port	TCP/IP port used to provide access for BOSS Smart Clients	23032
PAGIS 2.5 Service Port	TCP/IP port used to provide access for LPCS (formerly PAGIS) for older mobile client versions	8090
PAGIS 3.0 Service Port	TCP/IP port used to provide access to various mobile client versions	23033
VES Image Port	TCP/IP port used to receive reads from 3M fixed cameras	10000
VES UDP Ping Port	UDP port used to receive keep alive ping messages from 3M fixed cameras	10010
VES Heartbeat Port	TCP/IP port used to receive heartbeat status messages from 3M fixed cameras	10005
VES Exceptions Port	TCP/IP port used to receive exceptions messages from 3M fixed cameras	10011
Smart Client Deployment	TCP/IP port used for BOSS client installations via BOSS server	32023
REST API Port	HTML port used for the communication between the BOSS service and newer versions of LPCS	8092

If the checkbox in front of the port name is left unchecked, the corresponding connection will be disabled.

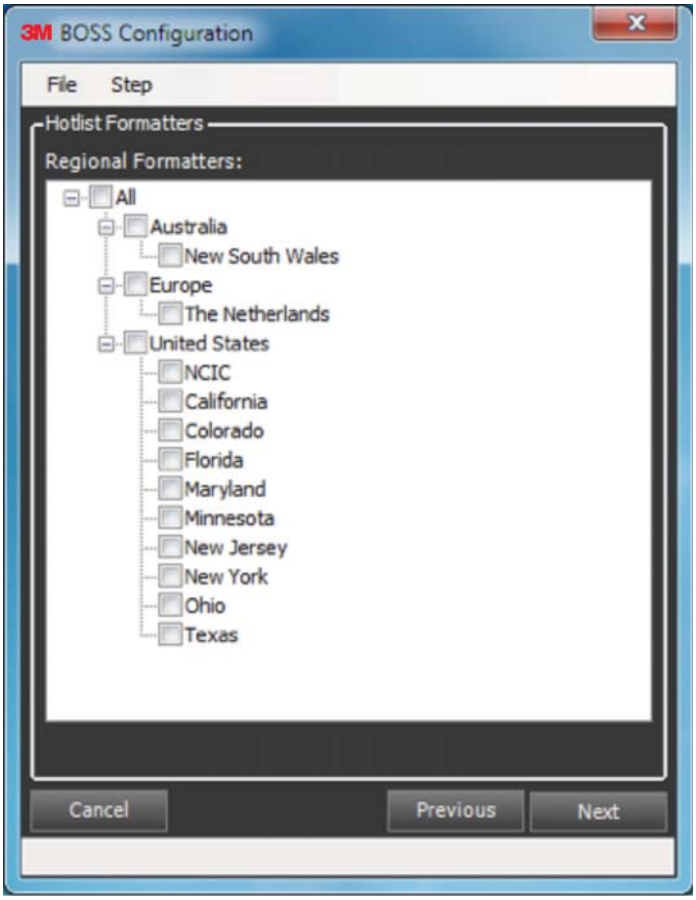
Smart Client Deployment Host – If this information is entered, BOSS Smart Clients will use the given hostname to distribute the smart client application. This can be left blank to use the local host name.

Firewall CIDR – BOSS provides a built-in firewall for incoming fixed camera connections. If a value is entered, only cameras with an IP address matching the CIDR will be allowed to connect. CIDR (Classless Inter-Domain Routing) is a standard industry method for specifying a range of included IP addresses. The format of the CIDR entry is A.B.C.D/N, in which the dotted decimal portion before the "/" is interpreted, like an IPv4 address, as a 32-bit binary number that has been broken into four octets. The value of N indicates the number of shared initial bits, counting from the left-hand side of the address.

For Example: For an entry of 10.200.200.255/24, the CIDR value 24 leaves 8 bits that can be changed. Therefore, addresses 10.200.200.x are permitted addresses.

SNTP Server – BOSS has a built-in time service. The 3M fixed ANPR/ALPR cameras do not support automatic daylight savings time (DST) adjustment. The BOSS time service provides a customized SNTP service for these cameras in order to support DST. To use the built-in time service, Windows Time Service has to be disabled in the Services Control panel, and the BOSS time server IP address entered in this field.

17.4.2.6 Regional Hotlist Formatters

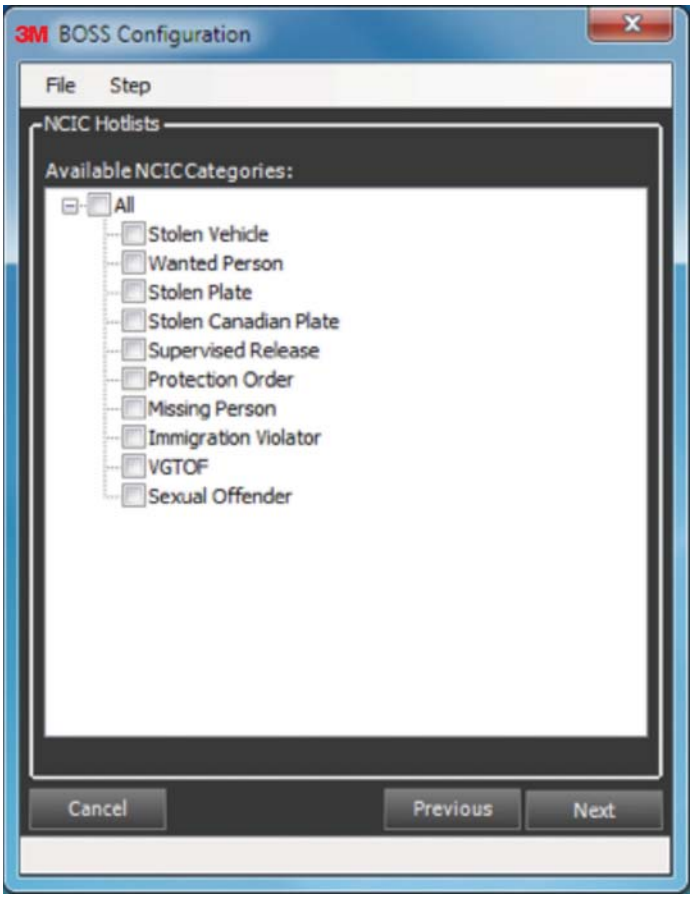


The BOSS 3.2 series allows the selection of predefined hotlist formatters. These formatters define the input format (structure) of hotlist data files. Custom formatters can be defined via the BOSS Smart Client application *(see Section 13 of this manual for more information).* Also, when installing BOSS in the United States, National Crime Information Center (NCIC) data formatters can be selected for specific states (see section following).

To select or unselect formatters, click on the formatter title to add or remove a check mark. Additional formatters can be added to a system as needed. These will be provided by 3M Technical Support upon request.

17.4.2.7 NCIC Hotlist Formatters

BOSS 3.2 and above supports hotlist import in the United States National Crime Information Center data format. This option is available only in the United States.



To configure formatters for the desired categories, check those categories.

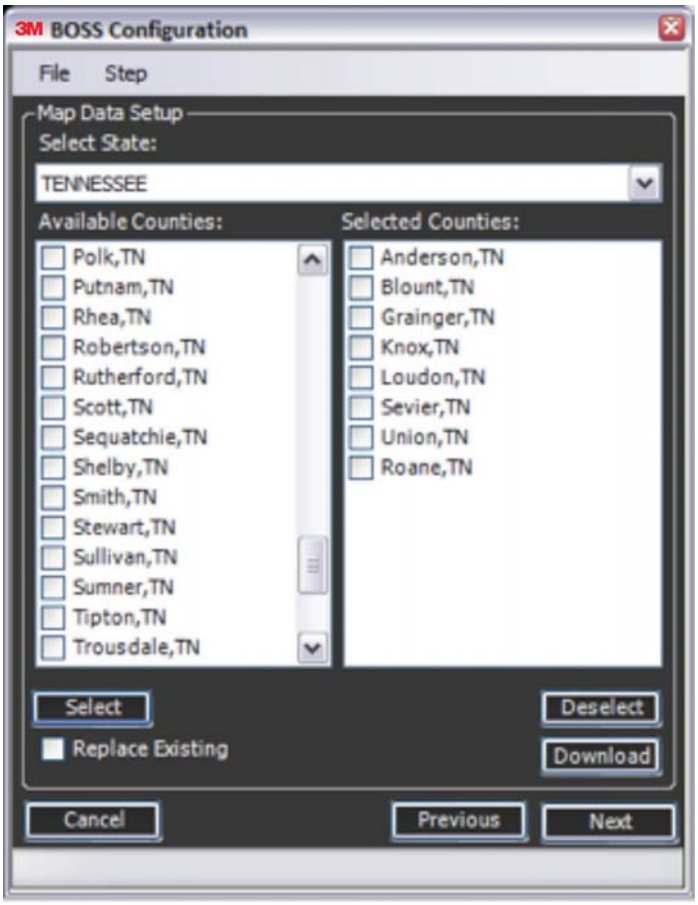
Once the desired categories have been selected, press **Next** to proceed.

17.4.2.8 TIGER Maps Configuration

BOSS 3.2 and above provides reporting on a map display by three alternative means. *See Section 17.3, Map Display Options with BOSS.* This option is available only in the United States.

Note: This section of configuration needs only be completed if U.S. Census Bureau TIGER maps are used.

BOSS provides for automated download of map data from the U.S. Census Bureau website. The U.S. Census Bureau offers yearly updated geographical information free of charge. In order to use TIGER maps, the BOSS server will need an established connection to the Internet **during the map download**. After the maps have been downloaded, the Internet connection is no longer needed.



To configure new maps for download:

1. Select the desired state from the drop-down menu. A list of counties for the selected state will appear.
2. Check the desired counties and click **Select.** Counties from multiple states can be selected

OR

3. Check undesired counties and click **Deselect.**

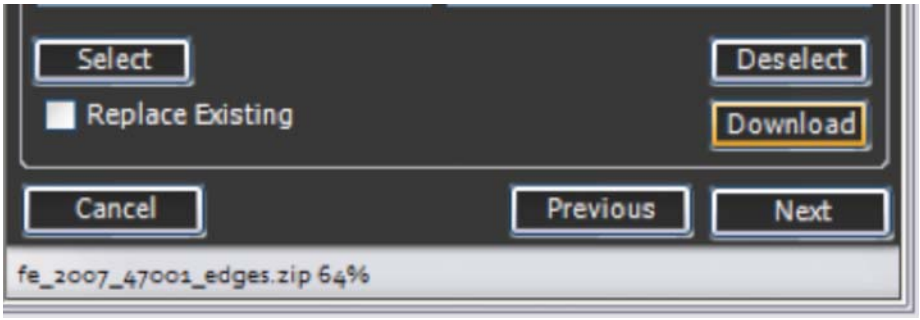
Once the desired counties have been selected:

4. Click **Download** to start the download process. BOSS will connect the U.S. Census Bureau website and extract the desired county data sets.

17.4.2.8 TIGER Maps Configuration *(continued)*

To replace existing maps:

BOSS maintains a copy of downloaded counties. To start anew and download a fresh set of data, check **Replace Existing** before clicking the **Download** button.

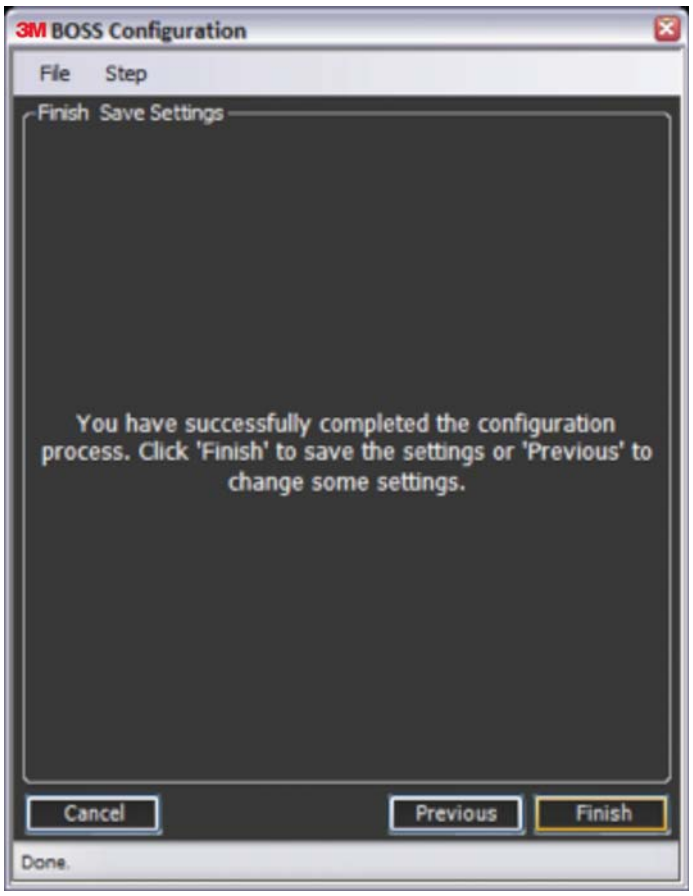


The status bar will indicate the download and extraction progress.

Note: The U.S. Census Bureau geospatial database has certain omissions and deficiencies. For more information, please consult the TIGER maps website: https://www.census.gov/geo/maps-data/data/tiger-line.html

---

17.4.2.9 Finishing Configuration



Click **Finish** to complete configuration. BOSS will save the chosen configuration.

If U.S. Census Bureau TIGER maps were downloaded, BOSS will prepare the map package to download to the Smart Clients. This may take several minutes. Progress will be displayed in the status bar.



Once the configuration process is complete, the Configuration Wizard will close automatically. In order to put the changed configuration in effect, the BOSS service will need to be restarted.

17.5 Installing the BOSS Smart Client Application

17.5.1 Installation over the Web

To initiate a web installation on a workstation, start up Microsoft Internet Explorer and navigate to this web address: **http://{boss_server_IP_address}:32023/publish.htm**, where {boss_server_IP_address} is the address of the server running the BOSS server application.

For Example: To install the Smart Client on the BOSS server itself, navigate to http://127.0.0.1:32023/publish.htm. The installation webpage will be presented. The advantage of installing the Smart Client over a web browser is that the application will automatically check for updated versions every time it is started.

17.5.2 Stand-Alone Installation

The BOSS Smart Client is a zero-administration desktop application meant for administration of the BOSS server application and querying data collected in the BOSS database as described in this manual. The BOSS Smart Client is installed as a single executable program. This program can be copied to any Windows workstation, or to a shared network drive.

To install the stand-alone application:

5. Start Windows Explorer on the BOSS server.
6. Navigate to the folder where the BOSS server application is installed (**by default C:\Program Files\PIPS Technology, Inc\BOSS3**)
7. Locate folder **sa_client.**
8. Copy file **BOSS.UI.exe** to the workstation or shared network folder of choice.

17.6 Configuring Client Tools

Client Tools is used to transfer any files needed during an LPCS shift from BOSS to an LPCS system that is being run in the Disk Sync mode. *See Section 13, Client Tools, and the License Plate Capture Software User's Manual.*

Client Tools does not have a customary interface. Once the utility is started, the Client Tools icon will appear in the Windows System Tray.

Before use, Client Tools must be configured and can be quickly completed with the simple configuration wizard provided:

1. To start the wizard, right-click the icon and select **Configure.** The initial screen provides information about the tool.
2. Click **Next** to continue the configuration, or **Cancel** to exit the wizard.
3. Enter a path so that Client Tools knows where to store the files it creates and where to look for files to process. This path can be a local, network, or external drive. Enter the path or click on the **…** button and browse to the location.
4. If the Begin Shift files that Client Tools creates need to be encrypted, click **Encrypt Output.** Click **Previous** to return to the previous screen, or click **Next** to continue.
5. The data used to create the Begin Shift files is created and managed in BOSS. Client Tools needs to know where the BOSS Server is located. Enter the server IP and the port to use to connect to it. Click **Previous** to return to the previous screen, or click **Next** to continue.
6. The final screen provides additional information on how to use the wizard. Click **Previous** to return to the previous screen, or click **Finish** to save the changes and exit.

17.7 The BOSS Upgrade Tool

If the BOSS application is upgraded to a newer version, the Upgrade Tool must be run before starting the BOSS Server. This tool is used to perform any database changes that may be necessary.

1. Navigate to the Upgrade tool. By default it is installed at **C:\Program Files (x86)\PIPS Technology, Inc\BOSS3\UpgradeTool.**
2. Right click on **BOSS3.UpgradeTool.exe** and select **Run as Administrator.**
3. When all processing is completed, click **Enter** to close the window.

18 Appendix: Troubleshooting

When troubleshooting an issue, always start by looking for error messages in the Server log file, usually found at …\PIPS Technology, Inc\BOSS3\logs\BOSSServerLog.txt. Proceed based on the following information, recognizing that escalation may be necessary. If so, obtain a copy of the complete error message and include it with all escalated documentation.

ISSUE REPORTED	EXPLANATION	STEPS TO CORRECT
Just after an installation/upgrade, the UI won't start.	It takes several moments for the BOSS Server to be completely started and ready for information to be accessed.	After starting the BOSS server, wait for several moments before attempting to start the UI. If this is an upgrade this could be several minutes while the database is being updated.
I start the BOSS Controller, but it stops a moment later. The following error message may display "Error: Error in BOSS3 Controller. Please check the log files." (New installation scenario)	The license was not activated. When checking the BOSS Server Log, there will be two error messages : – 'Licensed for 0 concurrent clients' and – 'Failed to set registry parameter [_tmpbalikeda63] to value System.Byte[].'	Return to the licensing activation and updating checklist. *(See Section 17.2, BOSS Version 3.2 and Above License Key Management.)*
I start the BOSS Controller, but it stops a moment later. The following error message may display "Error: Error in BOSS3 Controller. Please check the log files." (Upgrade scenario)	The Upgrade Tool must be run before starting the Controller.	Run the Upgrade Tool. *(See Section 17.7 The BOSS Upgrade Tool.)*
I start the BOSS Controller, but it stops a moment later. The following error message may display "Error: Error in BOSS3 Controller. Please check the log files." (Other scenario)	If the Upgrade Tool has been run, there may be a problem with the database.	Look for error messages in the BOSS Server Log. Provide this information to Technical Support.
A fixed camera won't connect.	The firewall could be blocking the communications.	Ensure that the firewall is allowing communications through the VES ports, found in the BOSS Configuration Controller on the Ports screen.
LPCS won't connect.	The firewall could be blocking the communications.	– Ensure that the firewall is allowing communications through the REST API (for LPCS 2.7.x) and PAGIS 3.0 Service (for versions of LPCS) ports, found in the BOSS Configuration Controller on the Ports screen. – Ensure that the device has been enabled in the BOSS UI Devices screen.
Hotlist will not update.	There is typically a problem with the source file.	– If it is a network hotlist, ensure that the site can be reached by entering the address in a browser. – If a local hotlist, ensure that the file is on the system and can be opened.

ISSUE REPORTED	EXPLANATION	STEPS TO CORRECT
The NCIC Hotlist formatter that I need is not available. (New installation scenario)	The NCIC formatters were not added during the initial installation.	Stop the BOSS Service. Go to the Configure option on the BOSS Controller. Step to the NCIC screen. Select the desired NCIC formatters. Click **Save** and exit. Restart the BOSS Service. The formatters will now be available.
I am unable to see reads/hits in the Dispatch screen.	The time on the read/hit coming in must be relatively close, within a couple of minutes, to the BOSS server time.	For a mobile ALPR system, correct the time on the laptop or ALPR processor. A fixed camera can be configured to use a time server. If issue persists, the server that BOSS is running on could also be configured to sync with a time server.
An error message, "Compressed method not supported," was found in the BOSS Server Log.	There is a problem with a source file for one of the hotlist.	Ensure that the source file can be opened. If not, update it with one that can be opened.
An error message, "Transaction has aborted," was found in the BOSS Server Log.	There are various reasons that this message can occur.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An error message. "Error #nn appeared in the db for Stored Procedure xxxx on line nn." was found in the BOSS Server Log.	An error occurred when running the stored procedure listed in the message.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An error message, "Timeout expired. The timeout period elapsed prior to completion of the operation or the server is not responding," was found in the BOSS Server Log.	A SQL timeout error has occurred.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An error message, "SNTP server not started, could not bind to InterNetwork 0.0.0.0:123," was found in the BOSS Server Log.	This is an expected error message that occurs when BOSS has not been configured to access a time server.	If no time server has been configured, this message can be ignored. If one has been configured, this needs to be escalated for further assistance.
After a new installation, the BOSS server stops running with an error message, "Failed in working with the database. Ensure connectivity is properly defined. Try running the BOSS Controller again and checking settings," was found in the BOSS Server Log.	When BOSS was started, there was a connection issue between it and the SQL Server.	Start by checking the information in the Controller. If that is all correct, then check to ensure that the SQL Server is running. If no issues are found there contact Technical Support Obtain a copy of the complete error message.
After a new installation, the BOSS Server stops with no error message in the BOSS Server Log.	The server needs to be run with Administrator privileges.	The server should be restarted in the Console as an Administrator. If running BOSS as a service then the BOSS Controller must be run as Administrator.
Error message in BOSS Server Log says that the file "httpconfig.exe" cannot be found.	This is an error that can occur when the system has not been updated in some time. It has been seen for other uncertain reasons as well.	Obtain a copy of the complete error message. Provide this information to Technical Support.

ISSUE REPORTED	EXPLANATION	STEPS TO CORRECT
After a new installation, the BOSS Server starts but stops moments later. The BOSS Server Log contains the error message. "The system cannot find the file specified Additional Exception Message: Unhandled exception from 'Name:BOSS3.exe. There are no context policies." However, no file is listed in the message.	This typically occurs on older systems, especially Windows Server 2003, or systems that have not been updated for a while.	The file **httpcfg.exe** needs to be copied into the c:\Windows\System32 directory.
The BOSS Server won't start, and there is an error message, "Transport Manager failed to listen on the supplied UIR using the NetTcpPortSharing service: failed to start the service because it is disabled," in the BOSS Server Log.	The NetTcpPortSharing Service is not running.	Obtain a copy of the complete error message. Provide this information to Technical Support.
The BOSS server stops running, and there is an error message, "Cannot open database "<Database Name>," in the BOSS Server Log.	There is an issue with the connection between the BOSS server and the SQL Server.	Start by checking the information in the Controller. If correct, then check to ensure that the SQL Server is running. If no issues are found contact Technical Support. Obtain a copy of the complete error message.
The BOSS Server won't start and there is an error message "A file activation error occurred. The physical file name '<filename>' may be incorrect." in the BOSS Server Log.	There could be multiple reasons, but it is probably due to a database connection issue.	Obtain a copy of the complete error message. Provide this information to Technical Support.
When running the upgrade tool, an error message is displayed. A message is included in the BOSS Server Log: "Current upgrade state: One of the upgrade scripts failed to run as expected. Please contact support for direction."	This most likely occurred due to upgrading from an old version of BOSS.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An unexpected response or behavior occurs in BOSS, and there is an error message, "Object reference not set to an instance of an object," in the BOSS Server Log.	This is a generic error message that can occur for various reasons.	Unless the issue has an obvious cause contact Technical Support. Obtain a copy of the complete error message.
The following error message, "Discarding tmp buffer because it's corrupted," has been found in the BOSS Server Log.	This message is associated with a database issue.	Obtain a copy of the complete error message. Provide the information to Technical Support.
The following error message, "SMTP server is not defined, email alerts disabled," has been found in the BOSS Server Log.	This message is informational indicating, as it states, that an email server has not been configured.	If attempts have been made to configure an email server and this error message occurs, recheck the settings and the server. If the error remains contact Technical Support.
The BOSS Service stops running, and the BOSS UI indicates that the server is not available. The following error message, "Cannot access a disposed object," is found in the BOSS UI Log.	This is an informational message provided by the UI confirming that it is no longer able to communicate with the BOSS server.	Restart the BOSS server and the BOSS UI will reconnect. If this does not correct the issue contact Technical Support.

ISSUE REPORTED	EXPLANATION	STEPS TO CORRECT
The following error message, “The socket connection was aborted,” is found in the BOSS UI Log.	This is an informational message provided by the UI confirming that it is no longer able to communicate with the BOSS server.	Restart the BOSS server, and the BOSS UI will reconnect. If this does not correct the issue contact Technical Support.
A problem occurs while adding a hotlist and the following error message “Invalid object name ‘<hotlist name here>’,” has been found in the BOSS Server Log.	This indicates that there is an issue with the hotlist formatter being used.	Confirm that the correct formatter is being used. If so, confirm the source file is formatted correctly. If so, contact Technical Support. Provide a copy of the full error message.
While installing BOSS, an error message displays: “Error opening file for writing: <File Name>.”	This indicates that the application listed in the error message is still running.	Check the Windows System Tray for any BOSS applications still running on the system. Close the application(s) and continue the installation.
The BOSS applications are installed under one user, but are not found when another user logs in.	The application was not installed using administrative privileges.	The application will need to be uninstalled and reinstalled using administrative privileges.
While using Client Tools to create Begin Shift files, an error message displays: “Client has not been activated on the server.”	Mobile devices must be enabled on BOSS to synchronize data to it. This message is displayed the first time that Client Tools is used to create Begin Shift files because it has not been enabled yet.	Configure Client Tools on BOSS *(see Section 17.6)* so that BOSS adds Client Tools as a device.
When using Client Tools to synchronize End Shift files to BOSS, the following error message displays: “Error: Could not find <file and path name>.”	Client Tools was unable to find the End Shift files to be processed at the defined path.	Check that the location assigned for the End Shift file matches the location chosen when Client Tools was configured. If it does not, move the file to the configured location.

19 Appendix: Plug-Ins

BOSS allows the use of third-party code via a plug-in that serves the needs of BOSS customers with specific data requirements. Once a plug-in is created and compiled, a copy of the DLL and any other necessary files can be copied to the plug-ins directory under BOSS. BOSS will automatically detect the existence of the plug-in at that point and permit reads to be passed to the ReceiveData method of your plug-in.

The functions of the currently available BOSS plug-ins are described in Sections 19.1 and 19.2. For more information and guidance on installing a plug-in, contact 3M Technical Support for guidance.

19.1 The BOSS Truck Drayage Utility

Regulation of diesel-fueled heavy-duty trucks and a Drayage Truck Registry (DTR) were implemented by the California Air Resources Board (ARB) to help reduce both emissions from these vehicles and public exposure to contaminants in those emissions. Drayage trucks subject to regulation (Class 7 and Class 8) are registered and information about them is maintained on an ARB web service.

The Truck Drayage Utility is BOSS plug-in that provides access to the ARB web service. The utility is designed to contact the web service, retrieve data, and add it to a comma-separated values file. In BOSS, the Hotlist Administrator will then create a whitelist that uses this CSV file as the source file.

The connection to the ARB web service (managed by the Windows Task Scheduler) can be made once daily for a full download of the data, with subsequent connections allowed no more frequently then every 30 minutes for updates. This whitelist can then be deployed to a mobile or fixed camera in the monitored area. If a plate is read that is not included on the whitelist, a notification will be displayed in BOSS. Appropriate action can be taken at that time.

If the ARB web service is unavailable and downloads cannot be completed, the BOSS whitelist will not be updated. There will also be warning messages in the BOSS log such as “Could not connect to <web service address>. TCP error code nnnnn: <Error description>.” If this occurs, the utility will try again in 30 minutes. If the errors persist, it may be necessary to seek assistance.

19.2 The BOSS LPRD Plug-in

The BOSS LPRD plug-in relays the reads the BOSS server receives on to the national database at the Automated Regional Justice Information System (ARJIS), a joint powers agency that facilitates information-sharing among more than 70 law enforcement agencies—local, state, and federal—in the two California counties (San Diego and Imperial) that border Mexico. ARJIS operates a secure intranet (ARJISnet) with more than 11,000 users in San Diego County alone.

19.3 The BOSS DEA Plug-in

The BOSS DEA plug-in writes LPR messages to the file system as reads are received by the BOSS server. Those files will then be available for the Drug Enforcement Agency, DEA, File Transporter to act upon.

20 Appendix: GNU Lesser General Public License

Version 2. 1, February 1999

Copyright ©1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages—typically libraries—of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are

the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a. The modified work must itself be a software library.

b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a “work that uses the Library”. Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a “work that uses the Library” with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a “work that uses the library”. The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a “work that uses the Library” uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a “work that uses the Library” with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer’s own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable “work that uses the Library”, as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user’s computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e. Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the “work that uses the Library” must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW.

EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Glossary

Term	Definition
ALPR	Automatic license plate recognition (also called automatic number plate recognition, or ANPR)
Annotation	A note or comment that can be made about and added to a read.
Deployment	The distribution or making available of a hotlist to a device
Device	A source of ALPR data; an LPCS unit or a fixed or mobile camera
Disposition	The classification of a hit; e.g., a recovered stolen vehicle
Fixed Camera	An ALPR camera permanently mounted above a roadway
Group	A group of BOSS users that belong together administratively
Hit	A match on a plate read against a hotlist
Hotlist	A list or database of license plates of interest, e.g., the NCIC database
Justification	A purpose for running a query on the captured data. There are several justifications included in the system by default. The BOSS Administrator can also create custom justifications to be used.
LPN	License plate number; also known as the Vehicle Plate Number
LPCS	3M™ License Plate Capture Software, the ALPR Mobile application
Local Server	A server running on a local system, in relation to the SQL server or the BOSS UI
Misread	A read that was marked as a misread by a user
Mobile Unit	An ALPR system with cameras, a mobile processor, and software, such as 3M License Plate Capture Software, installed in a vehicle
Notification	Propagation or delivery of an alert resulting from a hit
Overview	A color image of the vehicle to which the license plate is attached
Patch	A small image of the license plate
Permission	Authorization to access specified functionality in BOSS
Read	A license plate detection event that results in the plate text optical recognition and pictures being taken
Remote Server	A BOSS server that is running in another location
Role	A position, such as Administrator, with the authorization to access specified functionality in BOSS
Site	A group of related devices
Translation	The interpretation from a word in English to a word in a selected language
User	An authorized BOSS user (with a username and password)
Whitelist	In BOSS a whitelist hit is the opposite of a hotlist hit. When a license plate read does not exist in an enabled whitelist database, the same Hits (Alert) screen will be displayed.

Index

A

Access Permissions · 13, 20
Accessing Remote BOSS Server · 27
Adding
  Dispositions · 62
  Hotlist Entries · 37
  Justifications · 70
Administrator Role · 67
Alerts · 41
Application Screen · 10
Archiving Data · 60

B

BOSS Configuration · 85
BOSS Home Screen · 11
BOSS Installation · 74
BOSS Upgrade Tool · 95
BOSS Version 3.2 Design · 6
Branding · 66

C

Cameras · 6, 23
Client Tools · 59, 94
Configuration · 74, 83, 90
Configuration Wizard · 85
Creating
  Favorites · 55
  Hotlists · 28
  Groups · 15
  Roles · 67
  Sites · 25
  Targets · 39
  New Users · 17

D

Data Archiving · 60
Data, Querying Stored · 46
Data Sharing · 27
Default Devices · 21
Default Groups · 15
Default Roles · 67
Defining
  Devices · 22
  Hotlist Data Sources · 30
Deleting
  Devices · 24
  Dispositions · 62
  Favorites · 56
  Groups · 16
  Hotlist Entries · 38
  Justifications · 70
  Roles · 67
  Sites · 25
  Targets · 39
  Users · 18
Devices · 21
Dispatch · 42

E

Editing Devices · 23
Editing Parameters · 63
Enabling and Disabling
  Devices · 23
  Hotlists · 35
External Data · 50

F

Favorites · 55
Formatters, Hotlist · 40

G

Groups · 15

H

Help Documentation · 12
Hits · 43
Hotlists · 28
Hotlists, Enabling and Disabling · 35
Hotlist Entries, Adding · 37
Hotlist Entries, Modifying · 35
Hotlist Formatters · 40

I

Image Display · 52
Installation · 74

J

Justifications · 70

L

Language · 18, 26, 68
License Plate Capture Software, Interface through Client Tools · 59, 94
Login · 8
Login Statistics Report · 58

M

Manual Entry · 44
Manual Read · 44
Map Display Options · 83
Microsoft Bing Mapping · 83
Misreads · 11
Monitored Devices · 42

N

National Crime Information Center (NCIC) Databases · 90

Q

Query Criteria · 47
Query Results · 47, 51
Querying Stored Data · 46
Quick Search · 46

P

Parameters, BOSS System · 63
Parameters, Editing · 63
Parent Groups · 16
Permission Levels · 13
Plug-Ins · 100
Port Settings · 87
Preferences, Changing User · 26

R

Reads · 28
Reads, Adding a Manual · 44
Reads, Correcting · 45
Reads, Querying · 46
Remote BOSS Queries · 27
Remote BOSS Server, Accessing Reports, System Reports, Viewing and Printing · 57
Review · 60
Roles · 14, 67

S

Sites · 24
System Settings · 61
System Reports · 57
System Requirements, Minimum · 71
System Requirements, Recommended · 72

T

Targets · 38
Technical Support · 4
TIGER Maps · 83, 90
Translations · 68
Troubleshooting · 96

U

Upgrade Tool · 95
Users , Creating · 17
Users, Deleting · 18
Users, Importing from Active Directory · 19

3M Traffic Safety and Security Division
3M Center
Building 235-3A-09
St. Paul, MN 55144 USA
Phone: 1-877-777-3571
Fax: 1-800-591-9293
Email: MVSSALPR@mmm.com
www.3M.com/mvss

Please recycle. Printed in USA.
© 3M 2014. Used under license in Canada. All rights reserved.

75-0302-4350-7



Budget and Planning Estimate

COPLINK Data Source Integration Services

Prepared for

Commonwealth of Massachusetts Executive Office of Public Safety and Security

August 8, 2016

IBM Contact:
Nancy Keena
nancykeena@us.ibm.com
520-437-3823

Note: This Budget and Planning Estimate is not a binding contract and cannot be executed.

1. Introduction

IBM Safer Planet Software Services is pleased to offer this Budget and Planning Estimate (B&PE) to Commonwealth of Massachusetts Executive Office of Public Safety and Security ("MSP") for IBM i2 COPLINK ("COPLINK") Data Source Integration Services. This document provides an estimate of the recommended professional services in order for IBM to assist you with this initiative.

Whether your project is simple or highly complex, utilizing an experienced team with proven abilities is crucial to a successful engagement. Our team is comprised of resources that specialize in the Safer Planet solution set they represent with many years of COPLINK Software Services experience. As such, they bring to any project an unparalleled depth of COPLINK knowledge and best practices, delivered with the backing of Product Development. This organizational tie to the developers of the software and the specialized skills of our consultants means a complete services solution direct from IBM.

While we will work with your staff to ensure we meet your expectations for this project, this Letter serves as a framework for a high level implementation plan, and allows you to establish a budget for services.

1.1 Our Mission

COPLINK Software Services is a uniquely skilled services organization within the IBM Software Group. IBM provides deep subject matter skills and expertise to ensure each engagement is delivered following and sharing COPLINK best practices.

The ultimate goal within COPLINK Services is to run successful projects that are on time and within budget. We are responsible for blending client, IBM and, when appropriate, partner resources into a team, and for ensuring that the team works together to effectively deliver services related to COPLINK products.

Additionally, we are responsible for providing our clients with price estimates and contracts. We want your project to be a positive interaction with IBM, thus paving the way for more successful interactions with IBM in the future.

COPLINK Software Services is pleased to provide you with this B&PE Letter that outlines the activities associated with your COPLINK initiative. We have identified key phases of the engagement with a focus on COPLINK Software Services roles.

2. Budget and Planning Estimate (BPE)

This BPE for IBM Software Services contains a preliminary planning estimate that can be used for project budgeting purposes. The estimate is based on presales information provided by you and is subject to change pending the inclusion of additional requirements or an increase in project scope.

A formal contract for services, called a Statement of Work (SOW), must be jointly developed and executed before beginning the project.

2.1 Proposed Project Scope

This B&PE describes the proposed scope of the project. In this project IBM will integrate the following data source(s) into the Massachusetts COPLINK Node:

Agency Name	Participating Agencies	Vendor Name	Product Name	Product RDBMS	Data Set Types
Boston PD	Boston PD	Custom	Custom	MS SQL	RMS

2.2 Key Assumptions

This B&PE and IBM's estimates are based on the following key assumptions. Changes to these assumptions could impact the pricing estimate.

a. The estimate of effort/price required for this project may vary based on further discussion between MSP and Safer Planet Software Services. **The estimate requires the full cooperation of the client in all aspects of the project in a timely manner, including providing prerequisites, data, attending meetings and validation sessions and completion of verification forms.**

b. Estimates of effort/pricing presented in this B&PE are limited to the professional services described herein and do not include:

   (1) Hardware, software products and maintenance.

   (2) The services to install or upgrade hardware, third party system software or third party application software components for Initial Production or development/test environments, unless specifically included.

   (3) Formal training.

   (4) Taxes, shipping or any other charges not specifically included.

c. COPLINK Software Services reserves the right to subcontract services to technically qualified Consultants.

d. Setting up the refresh method may require any of the below, which MSP agrees to:

   (1) The installation of a database on your source instance and/or creation of tables into your source database.

   (2) Installation of triggers on your source database.

   (3) Replication of your database to a new database to track changes, and another SQL instance if replication of your database is the chosen refresh method.

e. Limited data cleaning will be provided. This data cleaning includes common “cleaning” functions such as standardizing record styles for names, addresses, criminal code and crime types. Data Cleaning does not include more intensive data restoration, to correct incomplete or incorrect records in the Data Source, or to standardize name, address or other data included in narrative reports. Intensive data restoration may be undertaken at ISP’s request as additional work scope at an additional charge, but will not be included under this B&PE.

f. Records included in the COPLINK data set are a subset of all available source data. Records not originally created by the application associated with the data source are considered “alien” and will not be mapped and migrated for inclusion in the COPLINK data set. For example, if incidents from an old RMS product were migrated into the database for a new RMS product that replaced it, those migrated incidents are considered to be “alien data.”

2.3 IBM Responsibilities

Under this B&PE, IBM will undertake the following activities:

Activity 1 - Project Management

IBM will provide project management for the IBM responsibilities in this B&PE through the IBM Project Manager. The purpose of this activity is to provide technical direction and control of IBM project personnel and to provide a framework for communications, reporting, procedural and contractual activity. This activity is composed of the following tasks:

Planning

a. Review the B&PE and the contractual responsibilities of both parties with your Project Manager.

b. Coordinate the establishment of the project environment.

c. Establish documentation and procedural standards for deliverable Materials.

d. Review with you the hardware required for the performance of this B&PE.

Project Tracking and Reporting

a. Review the IBM standard invoice format and billing procedure to be used on the project, with your Project Manager.

b. Administer the Project Change Control Procedure with your Project Manager.

c. Coordinate and manage the technical activities of IBM project personnel.

Completion Criteria:

This is an ongoing activity which will be considered complete at the end of the Services.

Deliverable Materials:

- None

Activity 2 - Project Kickoff

The purpose of this activity is to facilitate a high-level project kickoff meeting for MSP participants for up to two (2) hours at a mutually agreed date and time.

In this activity, IBM will perform Services which include the following tasks:

a. Introduce the project participants and Agencies;

b. Discuss project team roles and responsibilities;

c. Review the Services objectives;

d. Provide an overview of the project methodology;

e. Review Client environment; and

f. Initiate the Services.

Completion Criteria:

This activity will be considered complete when IBM has conducted the project kickoff meeting.

Deliverable Materials:

- None

Activity 3 - Data Analysis, Mapping and Conversion

The purpose of this activity is to extract information from the participating Agency Data Sources and migrate and integrate that data to create the COPLINK Database within the COPLINK Node.

IBM will:

a. Provide Client with a data storage device (encrypted USB drives) for each participating Agency to download their Data Source information onto and returned to IBM.

b. Provide an interface to connect to the vendor database on which the Agency Data Source information resides to provide access to such information.

c. Transfer each participating Agency's Data Source information and Data Source database structures from the data storage device to IBM servers.

d. Verify and analyze the transferred Agency Data Source information and Data Source database structures.

e. Map the Agency Data Source information to the COPLINK Database, including the mapping of Agency data codes to COPLINK Database codes.

f. Standardize and consolidate the Agency Data Source information into a Data Set to be stored in the COPLINK Database.

g. Migrate the Agency Data Source information, including the Data Set, Document Description, and Entity Description information, as listed in the tables in Appendix B, into the COPLINK Database.

Completion Criteria:

This activity will be complete when IBM has migrated the Agency Data Source information into the COPLINK Database.

Deliverable Materials:

- None

Activity 4 - Provide Data Migrator

In this activity, IBM will provide the Data Migrator to client on the Migration Server***.***

Delivery Location: IBM will deliver the Data Migrator electronically to the Client location. IBM personnel will install and configure Data Migrator on the existing Migration Server; it may not be deployed elsewhere

Open Source Software: Data Migrator may include open source software ("OSS"), which is not licensed by IBM. Your use of that OSS in connection with Data Migrator is subject to any and all requirements specified by the licenses of those open source materials. These licenses are detailed in the NOTICES.txt file included with Data Migrator.

Completion Criteria:

This activity will be complete when IBM has installed and configured Data Migrator as described above.

Deliverable Materials:

- None

Activity 5 - Data Merge and Data Refresh

In this activity, IBM will:

a. Compete the COPLINK data source migration by merging the data to the node; and

b. Enable the COPLINK refresh.

2.4 Your Responsibilities

The completion of the effort depends on the full commitment and participation of your management and personnel.

The responsibilities listed in this section are to be provided at no charge to IBM. IBM's performance is predicated upon the following responsibilities being fulfilled by you, as scheduled in the project plan. Delays in performance of these responsibilities may result in additional cost and/or delay of the completion of the project.

a. Designate a person called your Project Manager who will be the focal point for IBM communications relative to this project and will have the authority to act on behalf of you in all matters regarding this project;

b. Make appropriate personnel available to assist IBM in the performance of its responsibilities;

c. Supply all prerequisite hardware and software to be used during the performance of this SOW. This does not include any hardware or software normally used by IBM consultants in the performance of their day-to-day responsibilities with IBM;

d. Provide information and materials IBM requires to provide the Services. IBM will not be responsible for any loss, damage, delay, or deficiencies in the Services arising from inaccurate, incomplete, or otherwise deficient information or materials supplied by you or on behalf of you;

e. Ensure that current maintenance, license, and other applicable agreements are in place with third parties whose work may affect IBM's ability to provide the Services. Unless specifically agreed to otherwise in writing, Client is responsible for the management and performance of the third parties, and for any third party hardware, software or communications equipment used in connection with the Services;

f. Be responsible for the identification of, interpretation of, and compliance with, any applicable laws, regulations, and statutes that affect your existing systems, applications, programs, or data to which IBM will have access during the Services, including applicable data privacy, export, import laws and regulations, and product safety and regulatory compliance for non-IBM products including those recommended by IBM. You are solely responsible for obtaining advice of legal counsel as to the compliance with such laws, and regulations;

g. Assign the following personnel for each Client Agency responsible for making decisions regarding the Agency Data Source information during the project kickoff meeting:

   (1) A command level decision maker

   (2) A records department administrator

   (3) A sworn law enforcement officer, who will also be a user of the COPLINK Node.

h. You are responsible for protecting Data Migrator from any access not authorized in this SOW and ensure that its use is limited to the services described in this SOW.

i. Meet the following prerequisites prior to the start of the IBM Services under this SOW:

   (1) Provide connectivity and remote access, via a VPN or other secure dialup access, to the COPLINK Node to be used by IBM for installation, testing and support purposes, to the extent allowed by MSP security policy and practices.

   (2) Provide a data network connection employing TCP/IP between all participating agencies, including the Hosting Agency and those listed in the table under Project Scope.

   (3) Provide the required floor space, rack space and facilities (including power; lighting; and connectivity) for the hardware to be installed for the Services under this SOW.

   (4) Provide the hardware and software listed in Appendix C.

   (5) Install and configure the hardware required for the Data Migrator, as specified elsewhere in this SOW.

   (6) With the exception of SQL software, install and configure the software required for the Data Migrator, as specified in Appendix C.

j. The following responsibilities apply to the Data Analysis, Mapping and Conversion. MSP will:

   (1) Prior to the start of the data analysis, mapping and conversion activity, provide the following to IBM for each vendor database product containing the Agency Data Source information:

(a) Return the completed technical questionnaire/checklist packet from each participating Agency to IBM;

(b) Database backup data (historical load) for the Agency Data Source information database;

(c) A second database backup upon request (at least one month after the first historical load is provided); and

(d) The Geographic Information System ("GIS") map shape files for geo-coding.

(2) If the Contributing Agency cannot meet the responsibilities listed above for an Agency Data Source database within 30 days of the kick off meeting, IBM reserves the right to remove that Agency Data Source database from the Participating Agency table. IBM will bill for all work completed up to the most recently stamped milestone.

(3) Ensure that all Agency Data Source databases are using a currently supported version of the database and that all Agency Data Source databases are kept current with support and maintenance. Unsupported or down-level Agency Data Source database will not be included in the data analysis, mapping and conversion activity under this SOW.

(4) Either (i) copy the Data Source information to an encrypted data storage device provided by IBM and ship the data storage device to IBM, or (ii) send a copy of the Data Source information to IBM via SFTP (Secure FTP).

k. Acknowledge that:

(1) IBM reserves the right to subcontract services to technically qualified Consultants.

(2) Some or all data sources may require purchasing tools or interfaces from the Vendor of the product. MSP is responsible for purchasing those if necessary, including any fees the Vendor may charge related to this project.

l. The following responsibilities apply to the Annual Support:

(1) Client will designate up to three (3) representatives to contact IBM with questions regarding COPLINK Node during the annual support period.

(2) Provide VPN and remote desktop access to the hardware comprising the COPLINK solution so that IBM can monitor and maintain as described in this B&PE.

(3) Keep the third party hardware and software used for the Intermediate Machine current with any fixes and upgrades during the period of annual support.

(4) Notify IBM of bulk operations to be performed on data sources.

m. Be responsible for any data and the content of any database, the selection and implementation of procedures and controls regarding its access and, use, backup and recovery and security integrity of the stored data. This security will also include any procedures necessary to safeguard the integrity and security of software and data used in the Services from access by unauthorized personnel; and

n. If IBM requires access to your production systems, provide the required hardware (either an assigned desktop or laptop system) for such access. Any hardware provided for this access will be secured at your location when not in use by IBM.

2.5 Estimated Charges

2.5.1 Fixed Price Services

This project will include fixed-price Services:

Milestone	Price

Activity 1-2: Project Management and Kickoff (upon completion of Project Kickoff)	$5,000.00
Activity 3: Upon Completion of Data Analysis, Mapping and Conversion	$23,300.00
Total Service Charge:	**$28,300.00**

The total for all of the above fixed price services is: **$28,300.00.** These prices do not include Travel & Living (T&L) expense or applicable taxes.

Travel and living expenses are not expected for this SOW. Should any travel to your facility under this SOW be required, estimated travel and living expenses will be paid by you and will be authorized through the procedure described in Appendix A-1: Project Change Control Procedure

This Budget and Planning Estimate will expire on November 5, 2016 unless extended in writing by IBM.



Budget and Planning Estimate

COPLINK Data Source Integration Services

Prepared for

Commonwealth of Massachusetts Executive Office of Public Safety and Security

August 1, 2016

IBM Contact:
Nancy Keena
nancykeena@us.ibm.com
520-869-3672

Note: This Budget and Planning Estimate is not a binding contract and cannot be executed.

1. Introduction

IBM Safer Planet Software Services is pleased to offer this Budget and Planning Estimate (B&PE) to Commonwealth of Massachusetts Executive Office of Public Safety and Security for IBM i2 COPLINK ("COPLINK") Data Source Integration Services. This document provides an estimate of the recommended professional services in order for IBM to assist you with this initiative.

Whether your project is simple or highly complex, utilizing an experienced team with proven abilities is crucial to a successful engagement. Our team is comprised of resources that specialize in the Safer Planet solution set they represent with many years of COPLINK Software Services experience. As such, they bring to any project an unparalleled depth of COPLINK knowledge and best practices, delivered with the backing of Product Development. This organizational tie to the developers of the software and the specialized skills of our consultants means a complete services solution direct from IBM.

While we will work with your staff to ensure we meet your expectations for this project, this Letter serves as a framework for a high level implementation plan, and allows you to establish a budget for services.

1.1 Our Mission

COPLINK Software Services is a uniquely skilled services organization within the IBM Software Group. IBM provides deep subject matter skills and expertise to ensure each engagement is delivered following and sharing COPLINK best practices.

The ultimate goal within COPLINK Services is to run successful projects that are on time and within budget. We are responsible for blending client, IBM and, when appropriate, partner resources into a team, and for ensuring that the team works together to effectively deliver services related to COPLINK products.

Additionally, we are responsible for providing our clients with price estimates and contracts. We want your project to be a positive interaction with IBM, thus paving the way for more successful interactions with IBM in the future.

COPLINK Software Services is pleased to provide you with this B&PE Letter that outlines the activities associated with your COPLINK initiative. We have identified key phases of the engagement with a focus on COPLINK Software Services roles.

2. Budget and Planning Estimate (BPE)

This BPE for IBM Software Services contains a preliminary planning estimate that can be used for project budgeting purposes. The estimate is based on presales information provided by you and is subject to change pending the inclusion of additional requirements or an increase in project scope.

A formal contract for services, called a Statement of Work (SOW), must be jointly developed and executed before beginning the project.

2.1 Proposed Project Scope

This B&PE describes the proposed scope of the project. In this project IBM will perform a limited integration of the following data source(s) into the Massachusetts COPLINK Node:

Agency Name	Vendor Name	Product RDBMS	Data Set Types
Massachusetts State Police	xFact	MS SQL	Citations

2.2 Key Assumptions

This B&PE and IBM's estimates are based on the following key assumptions. Changes to these assumptions could impact the pricing estimate.

a. The estimate of effort/price required for this project may vary based on further discussion between Client and Safer Planet Software Services. **The estimate requires the full cooperation of the client in all aspects of the project in a timely manner, including providing prerequisites, data, and attending meetings.**

b. Estimates of effort/pricing presented in this B&PE are limited expressly to the professional services described herein and do not include:

   (1) Hardware, software products and maintenance.

   (2) The services to install or upgrade hardware, third party system software or third party application software components for Initial Production or development/test environments, unless specifically included.

   (3) Formal training.

   (4) Taxes, shipping or any other charges not specifically included.

c. Only the specific documents, elements and entities listed will be integrated. IBM can arrange for customizations at an additional charge.

d. Setting up the refresh method may require any of the below, which Massachusetts State Police agrees to:

   (1) The installation of a database on your source instance and/or creation of tables into your source database.

   (2) Installation of triggers on your source database.

   (3) Replication of your database to a new database to track changes, and another SQL instance if replication of your database is the chosen refresh method.

e. No data cleaning will be provided. This data cleaning includes common “cleaning” functions such as standardizing record styles for names, addresses, criminal code and crime types.

f. IBM will integrate a maximum of 1 million records or three (3) years of data, whichever limit is reached first.

g. Records included in the COPLINK data set are a subset of all available source data. Records not originally created by the application associated with the data source are considered “alien” and will not be mapped and migrated for inclusion in the COPLINK data set. For example, if incidents from an old RMS product were migrated into the database for a new RMS product that replaced it, those migrated incidents are considered to be “alien data.”

2.3 IBM Responsibilities

Under this B&PE, IBM will undertake the following activities:

Activity 1 - Project Management

IBM will provide project management for the IBM responsibilities in this B&PE through the IBM Project Manager. The purpose of this activity is to provide technical direction and control of IBM project personnel and to provide a framework for project planning, communications, reporting, procedural and contractual activity. This activity is composed of the following tasks:

Planning

a. Review the B&PE and the contractual responsibilities of both parties with your Project Manager.

b. Maintain project communications through your Project Manager.

c. Coordinate the establishment of the project environment.

d. Establish documentation and procedural standards for deliverable Materials.

e. Assist your Project Manager to prepare and maintain the project plan for the performance of this B&PE which will include the activities, tasks, assignments, milestones and estimates.

f. Review with you the hardware required for the performance of this B&PE.

Project Tracking and Reporting

a. Review project tasks, schedules, and resources and make changes or additions, as appropriate. Measure and evaluate progress against the project plan with your Project Manager.

b. Review the IBM standard invoice format and billing procedure to be used on the project, with your Project Manager.

c. Work with your Project Manager to address and resolve deviations from the project plan.

d. Administer the Project Change Control Procedure with your Project Manager.

e. Coordinate and manage the technical activities of IBM project personnel.

Completion Criteria:

This is an ongoing activity which will be considered complete at the end of the Services.

Deliverable Materials:

- None

Activity 2 - Project Kickoff

The purpose of this activity is to facilitate a high-level project kickoff meeting for Client participants for up to two (2) hours at a mutually agreed date and time.

In this activity, IBM will perform Services which include the following tasks:

a. Introduce the project participants and Agencies;

b. Discuss project team roles and responsibilities;

c. Review the Services objectives;

d. Provide an overview of the project methodology;

e. Provide Client with a technical questionnaire/checklist packet to be completed by the participating Agency, as listed in the table above in Project Scope;

f. Review Client environment;

g. Develop a preliminary schedule of activities; and

h. Initiate the Services.

Completion Criteria:

This activity will be considered complete when IBM has conducted the project kickoff meeting.

Deliverable Materials:

- Technical Questionnaire/Checklist
- High-level Timeline

Activity 3 - Data Analysis, Mapping and Conversion

The purpose of this activity is to extract information from the participating Agency Data Sources and migrate and integrate that data to create the COPLINK Database within the COPLINK Node.

IBM will:

a. Provide Client with a data storage device (encrypted USB drives) for each participating Agency to download their Data Source information onto and returned to IBM.

b. Provide an interface to connect to the vendor database on which the Agency Data Source information resides to provide access to such information.

c. Transfer each participating Agency's Data Source information and Data Source database structures from the data storage device to IBM servers.

d. Verify and analyze the transferred Agency Data Source information and Data Source database structures.

e. Map the Agency Data Source information to the COPLINK Database, including the mapping of Agency data codes to COPLINK Database codes.

f. Standardize and consolidate the Agency Data Source information into a Data Set to be stored in the COPLINK Database.

g. Migrate the Agency Data Source information, including the Data Set, Document Description, and Entity Description information, as listed in the tables in Appendix B, into the COPLINK Database.

Completion Criteria:

This activity will be complete when IBM has migrated the Agency Data Source information into the COPLINK Database.

Deliverable Materials:

- None

Activity 4 - Intermediate Machine Configuration and Testing

The purpose of this activity is to provide and configure certain hardware and software, as listed in Appendix B.

IBM will:

a. Remotely install and configure the SQL server software listed in Appendix B.

b. Perform System Test to validate the hardware and software is ready for Data Migration.

Completion Criteria:

This activity will be complete when IBM has provided the System Test Report describing online status of the hardware and software installation.

Deliverable Materials:

- None

Activity 5 - Provide Data Migrator

In this activity, IBM will provide the Data Migrator to Client on the Intermediate Machine (iBox).

Delivery Location: IBM will deliver the Data Migrator electronically to the Client location. IBM personnel will install and configure Data Migrator on the Intermediate Machine (iBox) described in Appendix B; it may not be deployed elsewhere

Open Source Software: Data Migrator may include open source software ("OSS"), which is not licensed by IBM. Your use of that OSS in connection with Data Migrator is subject to any and all

requirements specified by the licenses of those open source materials. These licenses are detailed in the NOTICES.txt file included with Data Migrator.

Completion Criteria:

This activity will be complete when IBM has installed and configured Data Migrator as described above.

Deliverable Materials:

- System Test Report

Activity 6 - Set up and Initiate Data Refresh

The purpose of this activity is to set and turn on the update method to ensure that adds, updates and deletes are being processed.

IBM will:

a. Set up the iBox or the database on the Client's RMS instance with the selected refresh method.

b. Start the refresh so that updates to the Client's database are processed into COPLINK.

Completion Criteria:

This activity will be complete when IBM has initiated the Data Refresh.

Deliverable Materials:

- Updated Refresh Report which shows new Data Source is Refreshing

2.4 Your Responsibilities

The completion of the effort depends on the full commitment and participation of your management and personnel.

The responsibilities listed in this section are to be provided at no charge to IBM. IBM's performance is predicated upon the following responsibilities being fulfilled by you, as scheduled in the project plan. Delays in performance of these responsibilities may result in additional cost and/or delay of the completion of the project.

a. Designate a person called your Project Manager who will be the focal point for IBM communications relative to this project and will have the authority to act on behalf of you in all matters regarding this project;

b. make appropriate personnel available to assist IBM in the performance of its responsibilities;

c. supply all prerequisite hardware and software to be used during the performance of this SOW. This does not include any hardware or software normally used by IBM consultants in the performance of their day-to-day responsibilities with IBM;

d. provide information and materials IBM requires to provide the Services. IBM will not be responsible for any loss, damage, delay, or deficiencies in the Services arising from inaccurate, incomplete, or otherwise deficient information or materials supplied by you or on behalf of you;

e. ensure that current maintenance, license, and other applicable agreements are in place with third parties whose work may affect IBM's ability to provide the Services. Unless specifically agreed to otherwise in writing, Client is responsible for the management and performance of the third parties, and for any third party hardware, software or communications equipment used in connection with the Services;

f. be responsible for the identification of, interpretation of, and compliance with, any applicable laws, regulations, and statutes that affect your existing systems, applications, programs, or

data to which IBM will have access during the Services, including applicable data privacy, export, import laws and regulations, and product safety and regulatory compliance for non-IBM products including those recommended by IBM. You are solely responsible for obtaining advice of legal counsel as to the compliance with such laws, and regulations;

g. assign the following personnel for each Client Agency responsible for making decisions regarding the Agency Data Source information during the project kickoff meeting and the integration process:

   (1) A command level decision maker

   (2) A records department administrator

   (3) A sworn law enforcement officer, who will also be a user of the COPLINK Node.

h. You are responsible for protecting Data Migrator from any access not authorized in this SOW and ensure that its use is limited to the services described in this SOW.

i. meet the following prerequisites prior to the start of the IBM Services under this SOW:

   (1) Provide connectivity and remote access, via a VPN or other secure dialup access, to the COPLINK Node to be used by IBM for installation, testing and support purposes, to the extent allowed by Client install and configure the software required for the Data Migrator, as specified in Appendix B.

j. The following responsibilities apply to the Data Analysis, Mapping and Conversion. Client will:

   (1) Prior to the start of the data analysis, mapping and conversion activity, provide the following to IBM for each vendor database product containing the Agency Data Source information:

      (a) return the completed technical questionnaire/checklist packet from each participating Agency to IBM;

      (b) database backup data (historical load) for the Agency Data Source information database;

      (c) a second database backup upon request (at least one month after the first historical load is provided); and

      (d) the Geographic Information System (“GIS”) map shape files for geo-coding.

   (2) If the Contributing Agency cannot meet the responsibilities listed above for an Agency Data Source database within 30 days of the kick off meeting, IBM reserves the right to remove that Agency Data Source database from the Participating Agency table. IBM will bill for all work completed up to the most recently stamped milestone.

   (3) Ensure that all Agency Data Source databases are using a currently supported version of the database and that all Agency Data Source databases are kept current with support and maintenance. Unsupported or down-level Agency Data Source database will not be included in the data analysis, mapping and conversion activity under this SOW.

   (4) Either (i) copy the Data Source information to an encrypted data storage device provided by IBM and ship the data storage device to IBM, or (ii) send a copy of the Data Source information to IBM via SFTP (Secure FTP).

k. Acknowledge that:

   (1) IBM reserves the right to subcontract services to technically qualified Consultants.

   (2) Client is responsible for any fees the Vendor security policy and practices.

(3) Provide a data network connection employing TCP/IP between all participating agencies, including the Hosting Agency and those listed in the table under Project Scope.

(4) Provide the required floor space, rack space and facilities (including power; lighting; and connectivity) for the hardware to be installed for the Services under this SOW.

(5) Provide the hardware and software listed in Appendix B.

(6) Install and configure the hardware required for the Data Migrator, as specified elsewhere in this SOW.

(7) With the exception of SQL software, may charge related to this project.

l. be responsible for any data and the content of any database, the selection and implementation of procedures and controls regarding its access and, use, backup and recovery and security integrity of the stored data. This security will also include any procedures necessary to safeguard the integrity and security of software and data used in the Services from access by unauthorized personnel; and

m. if IBM requires access to your production systems, provide the required hardware (either an assigned desktop or laptop system) for such access. Any hardware provided for this access will be secured at your location when not in use by IBM.

2.5 Estimated Charges

2.5.1 Fixed Price Services

This project will include fixed-price Services.

Milestone	Price
Activity 1-2: Project Management and Kickoff (upon completion of Project Kickoff)	$4,000.00
Activity 4-5: Upon Completion of Intermediate Machine Configuration and Testing & Provision of Data Migrator	$2,500.00
Activity 6: Upon Completion of Set up and Initiation of Data Refresh	$13,350.00
Total Service Charge:	**$19,850.00**

The total for all of the above fixed price services is $19,850.00. These prices do not include Travel & Living (T&L) expense or applicable taxes.

Travel and living expenses are not expected for this SOW. Should any travel to your facility under this SOW be required, estimated travel and living expenses will be paid by you and will be authorized through the a Project Change Procedure.

This Budget and Planning Estimate will expire on October 30, 2016 unless extended in writing by IBM.

Appendix A: Agency Source Data information Tables

The following table Lists the Documents, Elements and Entities included in this Estimate.

Agency Data Source Data Sets Description		
Client Agency Data Set Type	**Data Migrated**	**Data Not Migrated**
Citation System	Citations	N/A

Agency Data Source Document Descriptions		
Document	**Description**	**Standard Data Elements Migrated**
Citations	Represent a judicial summons issued to a person by a law enforcement official as the result of a minor occurrence, typically in response to a traffic infraction or misdemeanor	Citation Time/Date Citation Type Citation Number Citation Charge

Entity Descriptions		
Entity	**Standard Data Elements Migrated**	**Data Elements Not Migrated**
Persons	Name Alias(s) Gender Date of Birth Height Weight Eye Color Hair Color Race Ethnicity Marks Modus Operandi (MO) Appearances Caution Flags Gang Members Registered Offenders Employer Operator License Number Social Security Number State ID FBI ID Local ID	Religion Education Level Skill Set Dependent/Custody Financial Need Status/Indigent Fingerprints Citizenship Status Marital Status Sexuality Languages Spoken
Organizations	Name Organization Type	N/A
Officers	Name Badge Number	Personal Information

Entity Descriptions		
Entity	**Standard Data Elements Migrated**	**Data Elements Not Migrated**
Vehicles	Vehicle Identification Number (VIN) Class Make Model Style Year Color License Plate	Vehicle Impounds
Weapons	Type Manufacture Type Serial Number Color	N/A
Properties	Category Type Size Make Model Color Serial Number Quantity	N/A
Securities	Type Issuer Serial Number Denomination Quantity Value	N/A
Phones	Phone Number	N/A
Locations	Latitude/Longitude Address	N/A

Entity / Document	Persons	Organizations	Officers	Vehicles	Weapons	Phones	Locations
Citations	Y	Y	Y	Y	Y	Y	Y
	Y = Yes, when available in the source system						

Appendix B: Third Party Hardware and Software

The following third party hardware and software (or their equivalents) is required for the Services. Client will provide this hardware and software.

THIRD PARTY HARDWARE	Intermediate Machine
Quantity	Per Data Source
Processor	Intel Core i5
Clock Speed	3.1Ghz
Memory	8GB, DDR2 Non-ECC SDRAM, 800Mhz
Hard Drive	2x500GB 7200 RPM SATA 3.0GB/s & 8MB DataBurst
Hard Drive Configuration	RAID-1
Operating System	Windows 8 or Windows 10 or Windows Server 2012
Redundant Power	No
Peripherals and Accessories	2U Shelf, 19" Rack shelf, 13" deep

THIRD PARTY SOFTWARE	Intermediate Machine
Third Party Software	notepad++, 7-zip, MS SQL Server 2014 Express



Budget and Planning Estimate
COPLINK Custom Development Services

Prepared for
Massachusetts State Police

September 27, 2016

IBM Contact:
Nancy Keena
nancykeena@us.ibm.com
520-437-3823

Note: This Budget and Planning Estimate is not a binding contract and cannot be executed.

1. Introduction

IBM Safer Planet Software Services is pleased to offer this Budget and Planning Estimate (B&PE) to Massachusetts State Police ("MSP") for IBM i2 COPLINK ("COPLINK") Custom Development Services. This document provides an estimate of the recommended professional services in order for IBM to assist you with this initiative.

Whether your project is simple or highly complex, utilizing an experienced team with proven abilities is crucial to a successful engagement. Our team is comprised of resources that specialize in the Safer Planet solution set they represent with many years of COPLINK Software Services experience. As such, they bring to any project an unparalleled depth of COPLINK knowledge and best practices, delivered with the backing of Product Development. This organizational tie to the developers of the software and the specialized skills of our consultants means a complete services solution direct from IBM.

While we will work with your staff to ensure we meet your expectations for this project, this Letter serves as a framework for a high level implementation plan, and allows you to establish a budget for services.

1.1 Our Mission

COPLINK Software Services is a uniquely skilled services organization within the IBM Software Group. IBM provides deep subject matter skills and expertise to ensure each engagement is delivered following and sharing COPLINK best practices.

The ultimate goal within COPLINK Services is to run successful projects that are on time and within budget. We are responsible for blending client, IBM and, when appropriate, partner resources into a team, and for ensuring that the team works together to effectively deliver services related to COPLINK products.

Additionally, we are responsible for providing our clients with price estimates and contracts. We want your project to be a positive interaction with IBM, thus paving the way for more successful interactions with IBM in the future.

COPLINK Software Services is pleased to provide you with this B&PE Letter that outlines the activities associated with your COPLINK initiative. We have identified key phases of the engagement with a focus on COPLINK Software Services roles.

2. Budget and Planning Estimate (BPE)

This BPE for IBM Software Services contains a preliminary planning estimate that can be used for project budgeting purposes. The estimate is based on presales information provided by you and is subject to change pending the inclusion of additional requirements or an increase in project scope.

A formal contract for services, called a Statement of Work (SOW), must be jointly developed and executed before beginning the project.

2.1 Proposed Project Scope

This B&PE describes the proposed scope of the project. In this project IBM will:

a. Adjust RMV Licenses Data Source Mapping
b. Adjust RMV Licenses Refresh Feed
c. Develop the CJIS Message Broker Connector
d. Deploy CJIS Message Broker Configuration
e. Verify & Test the deployed solution

2.2 Key Assumptions

This B&PE and IBM's estimates are based on the following key assumptions. Changes to these assumptions could impact the pricing estimate.

a. The estimate of effort/price required for this project may vary based on further discussion between MSP and Safer Planet Software Services. **The estimate requires the full cooperation of the client in all aspects of the project in a timely manner, including providing prerequisites, data, attending meetings and validation sessions and completion of verification forms.**

b. Estimates of effort/pricing presented in this B&PE are limited to the professional services described herein and do not include:

   (1) Hardware, software products and maintenance.

   (2) The services to install or upgrade hardware, third party system software or third party application software components for Initial Production or development/test environments, unless specifically included.

   (3) Formal training.

   (4) Taxes, shipping or any other charges not specifically included.

c. COPLINK Software Services reserves the right to subcontract services to technically qualified Consultants.

2.3 IBM Responsibilities

Under this B&PE, IBM will undertake the following activities:

Activity 1 - Project Management

IBM will provide project management for the IBM responsibilities in this B&PE through the IBM Project Manager. The purpose of this activity is to provide technical direction and control of IBM project personnel and to provide a framework for project planning, communications, reporting, procedural and contractual activity. This activity is composed of the following tasks:

Planning

a. Review the B&PE and the contractual responsibilities of both parties with your Project Manager.

b. Maintain project communications through your Project Manager.

c. Coordinate the establishment of the project environment.

d. Establish documentation and procedural standards for deliverable Materials.

e. Assist your Project Manager to prepare and maintain the project plan for the performance of this B&PE which will include the product training plan, activities, tasks, assignments, milestones and estimates.

f. Review with you the hardware required for the performance of this B&PE.

Project Tracking and Reporting

a. Review project tasks, schedules, and resources and make changes or additions, as appropriate. Measure and evaluate progress against the project plan with your Project Manager.

b. Review the IBM standard invoice format and billing procedure to be used on the project, with your Project Manager.

c. Work with your Project Manager to address and resolve deviations from the project plan.

d. Participate in regularly scheduled project status meetings.

e. Prepare and submit periodic Status Reports to your Project Manager.

f. Administer the Project Change Control Procedure with your Project Manager.

g. Coordinate and manage the technical activities of IBM project personnel.

Completion Criteria:

This is an ongoing activity which will be considered complete at the end of the Services.

Deliverable Materials:

- Status Report(s)

Activity 2 - Project Kickoff

The purpose of this activity is to facilitate a high-level project kickoff meeting for MSP participants for up to two (2) hours at a mutually agreed date and time.

In this activity, IBM will perform Services which include the following tasks:

a. Introduce the project participants and Agencies;

b. Discuss project team roles and responsibilities;

c. Review the Services objectives;

d. Provide an overview of the project methodology;

e. Review Client environment;

f. Develop a preliminary schedule of activities; and

g. Initiate the Services.

Completion Criteria:

This activity will be considered complete when IBM has conducted the project kickoff meeting.

Deliverable Materials:

- High-level Timeline

Activity 3 - RMV Licenses Data Source Mapping Alteration

The purpose of this activity is to extract information from the RMV Licenses data source that is critical to the functioning of the CJIS Message Broker Connector.

IBM will:

a. Adjust the current data source mapping to add the source “PersonRMVSurrogateID” field to the COPLINK mapping. This value will be mapped to the DESCID table with a new L_IDTYPE value. This value will exist within the COPLINK Database solely for the CJIS Message Broker Connector functionality and will not be exposed to the end user.

Completion Criteria:

This activity will be complete when IBM has mapped the “PersonRMVSurrogateID” field to a DESCID and made the new L_IDTYPE value.

Deliverable Materials:

- None

Activity 4 - RMV Licenses Refresh Feed Alteration

The purpose of this activity is to alter the refresh feed for the RMV Licenses data source to propagate the new mapping of data critical to the CJIS Message Broker Connector functionality.

IBM will:

a. Deploy the updated mapping configuration for RMV Licenses.

b. Perform a full run of data in order to backfill all "PersonRMVSurrogateID" data into the COPLINK database.

c. Re-institute previous refresh method of calculating daily deltas and only pushing Adds, Updates, and Deletes of data.

Completion Criteria:

This activity will be complete when IBM has populated the node COPLINK database with "PersonRMVSurrogateID" data.

Deliverable Materials:

- None

Activity 5 - Develop the CJIS Message Broker Connector

The purpose of this activity is to execute the customer software development of the CJIS Message Broker Connector.

IBM will:

a. Enhance the COPLINK Server such that a new path will be created for gathering images for a Person details page. This path will check to see if there is an existing image available for a person and if not, attempt to retrieve a mug shot from the RMV via the CJIS Broker.

b. Enhance the COPLINK Search API to facilitate the same functionality as point "a" above.

c. Enhance the JNLP and Web Client such that they are able to display images from the RMV source.

Completion Criteria:

This activity will be complete when IBM has created the CJIS Message Broker and it has passed internal QA testing

Deliverable Materials:

- None

Activity 6 - Deploy CJIS Message Broker Configuration

In this activity, IBM will deploy the CJIS Message Broker to the node and make any necessary configuration changes to the node.

IBM will:

a. Remotely install and configure the CJIS Message Broker

b. Update any Node Configuration items that are required for the CJIS Message broker Functionality.

Completion Criteria:

This activity will be complete when IBM has installed and configured the CJIS Message Broker.

Deliverable Materials:

- None

Activity 7 - Verify and Test the Deployed Solution

The purpose of this activity is to verify and test the CJIS Message Broker functionality at the Node level and to ensure an end-user has the ability to see RMV images from a Person Details screen within COPLINK.

IBM will for both the JNLP and the Web Client:

a. Initiate a Person Search for a person that exists within the RMV Licenses data.

b. Drill down to the Person Details screen.

c. Verify the ability to view and image from the RMV service.

Completion Criteria:

This activity will be complete when IBM has provided the System Test form to your Project Manager.

Deliverable Materials:

- System Test Form

2.4 Your Responsibilities

The completion of the effort depends on the full commitment and participation of your management and personnel.

The responsibilities listed in this section are to be provided at no charge to IBM. IBM's performance is predicated upon the following responsibilities being fulfilled by you, as scheduled in the project plan. Delays in performance of these responsibilities may result in additional cost and/or delay of the completion of the project.

a. Designate a person called your Project Manager who will be the focal point for IBM communications relative to this project and will have the authority to act on behalf of you in all matters regarding this project;

b. make appropriate personnel available to assist IBM in the performance of its responsibilities;

c. supply all prerequisite hardware and software to be used during the performance of this SOW. This does not include any hardware or software normally used by IBM consultants in the performance of their day-to-day responsibilities with IBM;

d. provide information and materials IBM requires to provide the Services. IBM will not be responsible for any loss, damage, delay, or deficiencies in the Services arising from inaccurate, incomplete, or otherwise deficient information or materials supplied by you or on behalf of you;

e. ensure that current maintenance, license, and other applicable agreements are in place with third parties whose work may affect IBM’s ability to provide the Services. Unless specifically agreed to otherwise in writing, Client is responsible for the management and performance of the third parties, and for any third party hardware, software or communications equipment used in connection with the Services;

f. be responsible for the identification of, interpretation of, and compliance with, any applicable laws, regulations, and statutes that affect your existing systems, applications, programs, or data to which IBM will have access during the Services, including applicable data privacy,

export, import laws and regulations, and product safety and regulatory compliance for non-IBM products including those recommended by IBM. You are solely responsible for obtaining advice of legal counsel as to the compliance with such laws, and regulations;

g. Acknowledge that:

(1) IBM reserves the right to subcontract services to technically qualified Consultants.

2.5 Estimated Charges

2.5.1 Fixed Price Services

This project will include fixed-price Services.

Milestone	Price
Activity 1-2: Project Management and Kickoff (upon completion of Project Kickoff)	$8,260.00
Activity 3-4: RMV Licenses Data Source Mapping Alteration & Refresh Feed Alteration	$9,250.00
Activity 5: Develop the CJIS Message Broker Connector	$25,250.00
Activity 6-7: Deploy the CJIS Message Broker Configuration & Verify and Test the Deployed Solution	$21,000.14
Total Service Charge:	**$63,760.14**

The total for all of the above fixed price services is **$63,760.14.** These prices do not include Travel & Living (T&L) expense or applicable taxes.

Travel and living expenses are not expected for this SOW. Should any travel to your facility under this SOW be required, estimated travel and living expenses will be paid by you and will be authorized through the procedure described in Appendix A-1: Project Change Control Procedure

This Budget and Planning Estimate will expire on December 20, 2016 unless extended in writing by IBM.



Budget and Planning Estimate

COPLINK Data Source Integration Services

Prepared for

Commonwealth of Massachusetts Executive Office of Public Safety and Security

August 8, 2016

IBM Contact:
Nancy Keena
nancykeena@us.ibm.com
520-437-3823

Note: This Budget and Planning Estimate is not a binding contract and cannot be executed.

1. Introduction

IBM Safer Planet Software Services is pleased to offer this Budget and Planning Estimate (B&PE) to Commonwealth of Massachusetts Executive Office of Public Safety and Security ("MSP") for IBM i2 COPLINK ("COPLINK") Data Source Integration Services. This document provides an estimate of the recommended professional services in order for IBM to assist you with this initiative.

Whether your project is simple or highly complex, utilizing an experienced team with proven abilities is crucial to a successful engagement. Our team is comprised of resources that specialize in the Safer Planet solution set they represent with many years of COPLINK Software Services experience. As such, they bring to any project an unparalleled depth of COPLINK knowledge and best practices, delivered with the backing of Product Development. This organizational tie to the developers of the software and the specialized skills of our consultants means a complete services solution direct from IBM.

While we will work with your staff to ensure we meet your expectations for this project, this Letter serves as a framework for a high level implementation plan, and allows you to establish a budget for services.

1.1 Our Mission

COPLINK Software Services is a uniquely skilled services organization within the IBM Software Group. IBM provides deep subject matter skills and expertise to ensure each engagement is delivered following and sharing COPLINK best practices.

The ultimate goal within COPLINK Services is to run successful projects that are on time and within budget. We are responsible for blending client, IBM and, when appropriate, partner resources into a team, and for ensuring that the team works together to effectively deliver services related to COPLINK products.

Additionally, we are responsible for providing our clients with price estimates and contracts. We want your project to be a positive interaction with IBM, thus paving the way for more successful interactions with IBM in the future.

COPLINK Software Services is pleased to provide you with this B&PE Letter that outlines the activities associated with your COPLINK initiative. We have identified key phases of the engagement with a focus on COPLINK Software Services roles.

2. Budget and Planning Estimate (BPE)

This BPE for IBM Software Services contains a preliminary planning estimate that can be used for project budgeting purposes. The estimate is based on presales information provided by you and is subject to change pending the inclusion of additional requirements or an increase in project scope.

A formal contract for services, called a Statement of Work (SOW), must be jointly developed and executed before beginning the project.

2.1 Proposed Project Scope

This B&PE describes the proposed scope of the project. In this project IBM will integrate the following data source(s) into the Massachusetts COPLINK Node:

Agency Name	Vendor Name	Product RDBMS	Data Set Types
Massachusetts Transit Police	Larimore	MSSQL	RMS

2.2 Key Assumptions

This B&PE and IBM's estimates are based on the following key assumptions. Changes to these assumptions could impact the pricing estimate.

a. The estimate of effort/price required for this project may vary based on further discussion between MSP and Safer Planet Software Services. **The estimate requires the full cooperation of the client in all aspects of the project in a timely manner, including providing prerequisites, data, attending meetings and validation sessions and completion of verification forms.**

b. Estimates of effort/pricing presented in this B&PE are limited to the professional services described herein and do not include:

   (1) Hardware, software products and maintenance.

   (2) The services to install or upgrade hardware, third party system software or third party application software components for Initial Production or development/test environments, unless specifically included.

   (3) Formal training.

   (4) Taxes, shipping or any other charges not specifically included.

c. COPLINK Software Services reserves the right to subcontract services to technically qualified Consultants.

d. This estimate ***requires*** the following, which MSP and the participating agency agrees to:

   (1) Installation of triggers on the source database.

e. This estimate is based on the assumption the **schema of the client database is the same as Brookline's**. If it is different then a new estimate will need to be created.

f. Limited data cleaning will be provided. This data cleaning includes common "cleaning" functions such as standardizing record styles for names, addresses, criminal code and crime types. Data Cleaning does not include more intensive data restoration, to correct incomplete or incorrect records in the Data Source, or to standardize name, address or other data included in narrative reports. Intensive data restoration may be undertaken at ISP's request as additional work scope at an additional charge, but will not be included under this B&PE.

g. Records included in the COPLINK data set are a subset of all available source data. Records not originally created by the application associated with the data source are considered "alien" and will not be mapped and migrated for inclusion in the COPLINK data set. For example, if incidents from an old RMS product were migrated into the database for a new RMS product that replaced it, those migrated incidents are considered to be "alien data."

2.3 IBM Responsibilities

Under this B&PE, IBM will undertake the following activities:

Activity 1 - Project Management

IBM will provide project management for the IBM responsibilities in this B&PE through the IBM Project Manager. The purpose of this activity is to provide technical direction and control of IBM project personnel and to provide a framework for project planning, communications, reporting, procedural and contractual activity. This activity is composed of the following tasks:

Planning

a. Review the B&PE and the contractual responsibilities of both parties with your Project Manager.

b. Maintain project communications through your Project Manager.

c. Coordinate the establishment of the project environment.

d. Establish documentation and procedural standards for deliverable Materials.

e. Assist your Project Manager to prepare and maintain the project plan for the performance of this B&PE which will include the product training plan, activities, tasks, assignments, milestones and estimates.

f. Review with you the hardware required for the performance of this B&PE.

Project Tracking and Reporting

a. Review project tasks, schedules, and resources and make changes or additions, as appropriate. Measure and evaluate progress against the project plan with your Project Manager.

b. Review the IBM standard invoice format and billing procedure to be used on the project, with your Project Manager.

c. Work with your Project Manager to address and resolve deviations from the project plan.

d. Participate in regularly scheduled project status meetings.

e. Prepare and submit periodic Status Reports to your Project Manager.

f. Administer the Project Change Control Procedure with your Project Manager.

g. Coordinate and manage the technical activities of IBM project personnel.

Completion Criteria:

This is an ongoing activity which will be considered complete at the end of the Services.

Deliverable Materials:

- Status Report(s)

Activity 2 - Project Kickoff

The purpose of this activity is to facilitate a high-level project kickoff meeting for MSP participants for up to two (2) hours at a mutually agreed date and time.

In this activity, IBM will perform Services which include the following tasks:

a. Introduce the project participants and Agencies;

b. Discuss project team roles and responsibilities;

c. Review the Services objectives;

d. Provide an overview of the project methodology;

e. Provide Client with a technical questionnaire/checklist packet to be completed by each participating Agency, as listed in the table above in Project Scope;

f. Provide a sample Memorandum of Understanding document for Client's use with its participating Agencies that will share their Data Source information, if required;

g. Review Client environment;

h. Develop a preliminary schedule of activities; and

i. Initiate the Services.

Completion Criteria:

This activity will be considered complete when IBM has conducted the project kickoff meeting.

Deliverable Materials:

- Technical Questionnaire/Checklist
- Sample Memorandum of Understanding, if required
- High-level Timeline

Activity 3 - Data Analysis, Mapping and Conversion

The purpose of this activity is to extract information from the participating Agency Data Sources and migrate and integrate that data to create the COPLINK Database within the COPLINK Node.

IBM will:

a. Provide Client with a data storage device (encrypted USB drives) for each participating Agency to download their Data Source information onto and returned to IBM.

b. Provide an interface to connect to the vendor database on which the Agency Data Source information resides to provide access to such information.

c. Transfer each participating Agency's Data Source information and Data Source database structures from the data storage device to IBM servers.

d. Verify and analyze the transferred Agency Data Source information and Data Source database structures.

e. Map the Agency Data Source information to the COPLINK Database, including the mapping of Agency data codes to COPLINK Database codes.

f. Standardize and consolidate the Agency Data Source information into a Data Set to be stored in the COPLINK Database.

g. Migrate the Agency Data Source information, including the Data Set, Document Description, and Entity Description information, as listed in the tables in Appendix B, into the COPLINK Database.

Completion Criteria:

This activity will be complete when IBM has migrated the Agency Data Source information into the COPLINK Database.

Deliverable Materials:

- None

Activity 4 - Data Verification and Data Review

The purpose of this activity is to work with MSP to validate and correct the Agency Data Source information that has been migrated into the COPLINK Database.

IBM will:

a. Select a sample set of documents from the Agency Data Source information, as determined by IBM with input from each participating Agency, to review and validate the conversion of the Agency Data Source information into the COPLINK Database.

b. Conduct, with assistance from Client, a side-by-side, field-by-field comparison of the selected sample set of documents, comparing the original documents from the Agency Data Source to those same documents migrated into the COPLINK Database.

c. Document any issues found as a "Blocking" issue or a "Non-blocking" issue and provide a tracking number for each issue found. A "Blocking" issue is one that will be resolved or a workaround provided prior to Data Verification. A "Non-blocking" issue is one that does not have to be resolved prior to Data Verification.

d. Resolve or provide a workaround for the identified Blocking issues.

e. Present the issue resolutions to Client and each Contributing Agency.

f. Provide Data Verification form to Client for sign-off.

Completion Criteria:

This activity will be complete when IBM has provided the Data Verification form to your Project Manager.

Deliverable Materials:

- Data Verification Form

Activity 5 - Provide Data Migrator

In this activity, IBM will provide the Data Migrator to MSP***.***

Delivery Location: IBM will deliver the Data Migrator electronically to the Client location. IBM personnel will install and configure Data Migrator on the Migration Server; it may not be deployed elsewhere

Open Source Software: Data Migrator may include open source software ("OSS"), which is not licensed by IBM. Your use of that OSS in connection with Data Migrator is subject to any and all requirements specified by the licenses of those open source materials. These licenses are detailed in the NOTICES.txt file included with Data Migrator.

Completion Criteria:

This activity will be complete when IBM has installed and configured Data Migrator as described above and turned on the refresh process.

Deliverable Materials:

- None

2.4 Your Responsibilities

The completion of the effort depends on the full commitment and participation of your management and personnel.

The responsibilities listed in this section are to be provided at no charge to IBM. IBM's performance is predicated upon the following responsibilities being fulfilled by you, as scheduled in the project plan. Delays in performance of these responsibilities may result in additional cost and/or delay of the completion of the project.

a. Designate a person called your Project Manager who will be the focal point for IBM communications relative to this project and will have the authority to act on behalf of you in all matters regarding this project;

b. Make appropriate personnel available to assist IBM in the performance of its responsibilities;

c. Supply all prerequisite hardware and software to be used during the performance of this SOW. This does not include any hardware or software normally used by IBM consultants in the performance of their day-to-day responsibilities with IBM;

d. Provide information and materials IBM requires to provide the Services. IBM will not be responsible for any loss, damage, delay, or deficiencies in the Services arising from inaccurate, incomplete, or otherwise deficient information or materials supplied by you or on behalf of you;

e. Ensure that current maintenance, license, and other applicable agreements are in place with third parties whose work may affect IBM's ability to provide the Services. Unless specifically agreed to otherwise in writing, Client is responsible for the management and performance of the third parties, and for any third party hardware, software or communications equipment used in connection with the Services;

f. Be responsible for the identification of, interpretation of, and compliance with, any applicable laws, regulations, and statutes that affect your existing systems, applications, programs, or data to which IBM will have access during the Services, including applicable data privacy, export, import laws and regulations, and product safety and regulatory compliance for non-IBM products including those recommended by IBM. You are solely responsible for obtaining advice of legal counsel as to the compliance with such laws, and regulations;

g. Assign the following personnel for each Client Agency responsible for making decisions regarding the Agency Data Source information during the project kickoff meeting and the Data Verification and Data Review activities:

(1) A command level decision maker

(2) A records department administrator

(3) A sworn law enforcement officer, who will also be a user of the COPLINK Node.

h. You are responsible for protecting Data Migrator from any access not authorized in this SOW and ensure that its use is limited to the services described in this SOW.

i. Meet the following prerequisites prior to the start of the IBM Services under this SOW:

(1) Provide connectivity and remote access, via a VPN or other secure dialup access, to the COPLINK Node to be used by IBM for installation, testing and support purposes, to the extent allowed by MSP security policy and practices.

(2) Provide a data network connection employing TCP/IP between all participating agencies, including the Hosting Agency and those listed in the table under Project Scope.

(3) Provide the required floor space, rack space and facilities (including power; lighting; and connectivity) for the hardware to be installed for the Services under this SOW.

(4) Provide the hardware and software listed in Appendix C.

j. The following responsibilities apply to the Data Analysis, Mapping and Conversion. MSP will:

(1) Prior to the start of the data analysis, mapping and conversion activity, provide the following to IBM for each vendor database product containing the Agency Data Source information:

(a) Return the completed technical questionnaire/checklist packet from each participating Agency to IBM;

(b) Database backup data (historical load) for the Agency Data Source information database;

(c) A second database backup upon request (at least one month after the first historical load is provided); and

(d) The Geographic Information System (“GIS”) map shape files for geo-coding.

(2) If the Contributing Agency cannot meet the responsibilities listed above for an Agency Data Source database within 30 days of the kick off meeting, IBM reserves the right to remove that Agency Data Source database from the Participating Agency table. IBM will bill for all work completed up to the most recently stamped milestone.

(3) Ensure that all Agency Data Source databases are using a currently supported version of the database and that all Agency Data Source databases are kept current with support and maintenance. Unsupported or down-level Agency Data Source database will not be included in the data analysis, mapping and conversion activity under this SOW.

(4) Either (i) copy the Data Source information to an encrypted data storage device provided by IBM and ship the data storage device to IBM, or (ii) send a copy of the Data Source information to IBM via SFTP (Secure FTP).

k. The following responsibilities apply to the Data Verification and Data Review. MSP will:

(1) Assist IBM as required with the side-by-side, field-by-field comparison of the selected sample set of documents, comparing the original documents from the Agency Data Source to those same documents migrated into the COPLINK Database.

(2) Make staff available for the data verification and review sessions within 48 hours of completion of the migration activity. IBM will have the right to invoice for this step and continue with the remainder of the project, if the resources are not made available within the time frame specified.

(3) Provide the completed, signed Data Verification form to IBM.

l. Acknowledge that:

(1) IBM reserves the right to subcontract services to technically qualified Consultants.

(2) Some or all data sources may require purchasing tools or interfaces from the Vendor of the product. MSP is responsible for purchasing those if necessary, including any fees the Vendor may charge related to this project.

m. Be responsible for any data and the content of any database, the selection and implementation of procedures and controls regarding its access and, use, backup and recovery and security integrity of the stored data. This security will also include any procedures necessary to safeguard the integrity and security of software and data used in the Services from access by unauthorized personnel; and

n. If IBM requires access to your production systems, provide the required hardware (either an assigned desktop or laptop system) for such access. Any hardware provided for this access will be secured at your location when not in use by IBM.

2.5 Estimated Charges

2.5.1 Fixed Price Services

This project will include fixed-price Services:

Milestone	Price
Activity 1-2: Project Management and Kickoff (upon completion of Project Kickoff)	$3,000.00
Activity 4: Upon Completion of Data Verification and Data Review	$13.500.00
Activity 5: Upon Completion of Provide Data Migrator	$2,300.00
Total Service Charge:	**$18,800.00**

The total for all of the above fixed price services is: **$18,800.00.** These prices do not include Travel & Living (T&L) expense or applicable taxes.

Travel and living expenses are not expected for this SOW. Should any travel to your facility under this SOW be required, estimated travel and living expenses will be paid by you and will be authorized through the procedure described in Appendix A-1: Project Change Control Procedure

This Budget and Planning Estimate will expire on November 5, 2016 unless extended in writing by IBM.

Appendix A: Agency Source Data information Tables

The following table if for reference only. The Data Set Type listed above is defined by the documents and entities included as outlined below.

Agency Data Source Data Sets Description		
Client Agency Data Set Type	**Standard Data Migrated**	**Data Not Migrated**
Records Management System (RMS)	Department Reports Supplemental Reports Traffic Collisions Miscellaneous Incident Citations Field Interviews Permits Pawns Supervisions (Registration) Supervisions (Court Ordered)	Jail Management System (JMS) data Mug Shots CAD data AFIS data Probation data Court data CJIS data Vehicle Tow data Intelligence documents Crime Analysis documents Civil Process documents Arraignments Watch Lists Motor Vehicle Dept. Images

Agency Data Source Document Descriptions		
Document	**Description**	**Standard Data Elements Migrated**
Departmental Reports	Records the occurrence of a crime, police action taken, or information that a law enforcement officer deems significant enough to create a permanent record of an incident	Incident Begin Time/Date Incident End Time/Date Report Number Beat Grid Crime Type(s) Arrest Type Arrest Number Arrest Charge
Supplemental Reports	Records activities of law enforcement officers as they continue to investigate a specific Departmental Report	Same as Departmental Reports
Traffic Collisions	Records a collision of one vehicle with another vehicle, person, or other object	Same as Departmental Reports
Miscellaneous Incidents	An abbreviated form of a report that describes a minor incident that does not require any follow-up investigation. This document type is created only in cases where Departmental Reports can be distinguished from Miscellaneous Reports	Same as Departmental Reports

Agency Data Source Document Descriptions		
Document	**Description**	**Standard Data Elements Migrated**
Citations	Represent a judicial summons issued to a person by a law enforcement official as the result of a minor occurrence, typically in response to a traffic infraction or misdemeanor	Citation Type Citation Number Citation Status Beat Grid Citation Charge
Field Interviews	Contain information about contact between a law enforcement officer and at least one individual for any activity an officer feels is suspicious	Field Interview Type Field Interview Number Beat Grid
Pawn Tickets	Contain information about persons and property involved in a pawn transaction	Pawn Ticket Number Pawn Shop Name
Permits	Represent permissions granted to an individual such as the privilege to carry a concealed weapon, a driver's license, or handicap parking permit	Permit Type Permit Number Permit Status Grid
Supervisions (Court Ordered)	An official proclamation by a judge that defines the legal relationship between the parties to a hearing, a trial, an appeal, or other court proceedings. Such ruling requires or authorizes the carrying out of certain steps by one or more parties to a case. Types of Court-Ordered Supervisions include: Community Supervision Drug Court Supervision Federal Court Supervision Juvenile Court Supervision Miscellaneous Court Supervision Prohibited Possessor (Firearm) Court Order of Protection Travel Restriction No Trespass Temporary Restraining Order Work Release Pre-Trial Release	Supervision Type Supervision Reference Number Supervision Start Date Supervision End Date Supervision Status
Supervisions (Registration)	Records the periodic registration of an individual who has been ordered by the court to report home location and other pertinent information as deemed by local law enforcement or the court. Types of Registration Supervisions include: Registered Gang Member Registered Arson Registered Felon Registered Repeat Offender Registered Sex Offender Registered Narcotic Offender	Supervision Type Supervision Reference Number Supervision Start Date Supervision End Date Supervision Status

Entity Descriptions		
Entity	**Standard Data Elements Migrated**	**Data Elements Not Migrated**
Persons	Name Alias(s) Gender Date of Birth Height Weight Eye Color Hair Color Race Ethnicity Marks Modus Operandi (MO) Appearances Caution Flags Gang Members Registered Offenders Employer Operator License Number Social Security Number State ID FBI ID Local ID	Religion Education Level Skill Set Dependent/Custody Financial Need Status/Indigent Fingerprints Citizenship Status Marital Status Sexuality Languages Spoken
Organizations	Name Organization Type	N/A
Officers	Name Badge Number	Personal Information
Vehicles	Vehicle Identification Number (VIN) Class Make Model Style Year Color License Plate	Vehicle Impounds
Weapons	Type Manufacture Type Serial Number Color	N/A
Properties	Category Type Size Make Model Color Serial Number Quantity	N/A

Entity Descriptions		
Entity	**Standard Data Elements Migrated**	**Data Elements Not Migrated**
Securities	Type Issuer Serial Number Denomination Quantity Value	N/A
Phones	Phone Number	N/A
Locations	Latitude/Longitude Address	N/A

Standard Entities Per Document									
Entity **Document**	**Persons**	**Organizations**	**Officers**	**Vehicles**	**Weapons**	**Properties**	**Securities**	**Phones**	**Locations**
Departmental Reports	Y	Y	Y	Y	Y	Y	Y	Y	Y
Supplemental Reports	Y	Y	Y	Y	Y	Y	Y	Y	Y
Traffic Collisions	Y	Y	Y	Y	Y	Y	Y	Y	Y
Miscellaneous Incidents	Y	Y	Y	Y	Y	Y	Y	Y	Y
Citations	Y	Y	Y	Y	Y	Y	Y	Y	Y
Field Interviews	Y		Y	Y				Y	Y
Pawn Tickets	Y	Y		Y	Y	Y		Y	Y
Permits	Y			Y	Y			Y	Y
Supervisions	Y	Y	Y					Y	Y
	Y = Yes, when available in the source system								

CONNECTICUT CVISN E-SCREENING and WIM SCREENING PILOT PROJECT

Trucks Impacts



Prepared for

Connecticut Department of Transportation,
Connecticut Department of Motor Vehicle &
CASE Study Committee

Prepared by

Barry Mason, BGM Consulting LLC

IMPACTS: Class 9, 5 Axle Truck 252

Truck Gross Weight	Approximate Impacts	Approximate Cars
80,000#	1 Truck	9600
90.000#	2 Trucks	19,200
100,000#	4 Trucks	38,400
110,000#	8 Trucks	76,800
120,000#	16 Trucks	153,600
130,000#	32 Trucks	307,200
140,000#	64 Trucks	614,400
150,000#	128 Trucks	1,228,800
160,000#	256 Trucks	2,457,600
170,000#	512 Trucks	4,915,200
180,000#	1024 Trucks	9,830,400
190,000#	2048 Trucks	19,660,800
200,000#	4096 Trucks	39,321,600

IMPACTS: Class 9, 5 Axle Truck 253

Vehicle Type	Speed	Braking Distance	Reaction Distance	Total Distance
Car	70MPH	245’	69’	314’
80K Truck	70MPH	456’	69’	525’
90K Truck	70MPH			
100K Truck	70MPH			
120K Trucks	70MPH			
130K Trucks	70MPH			
140K Trucks	70MPH			
150K Trucks	70MPH			
160K Trucks	70MPH			

Smart Roadside & Drivewyze Technologies

Connecticut Academy of Science and Engineering (CASE)
May 24th, 2017



iis

Who We Are

- IIS is a company dedicated and focused on Commercial Vehicle Enforcement (CVE), Commercial Vehicle Operations (CVO) and Freight Mobility
- Unparalleled track record of delivering successful e-screening (F, V & M) & V2I solutions
- Solid History of Performance, bringing high value, award winning solutions to all of our Agency Partners
- In-house dedicated teams in Sensors, Systems, IT Systems, Field Deployment and Maintenance

Vision

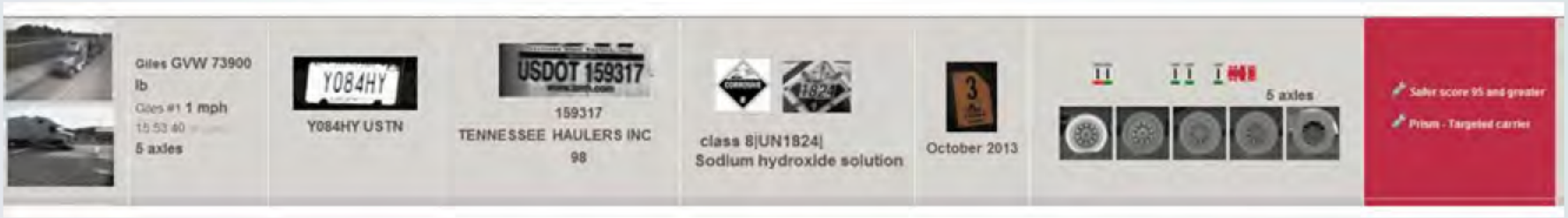
A safe and efficient commercial vehicle transportation system with zero crashes and zero fatalities.

Smart Roadside Technologies

Smart Roadside is the **leading** safety & enforcement platform **proven** to deliver agencies **measurable outcomes.**

Smart Roadside Screening (SW)

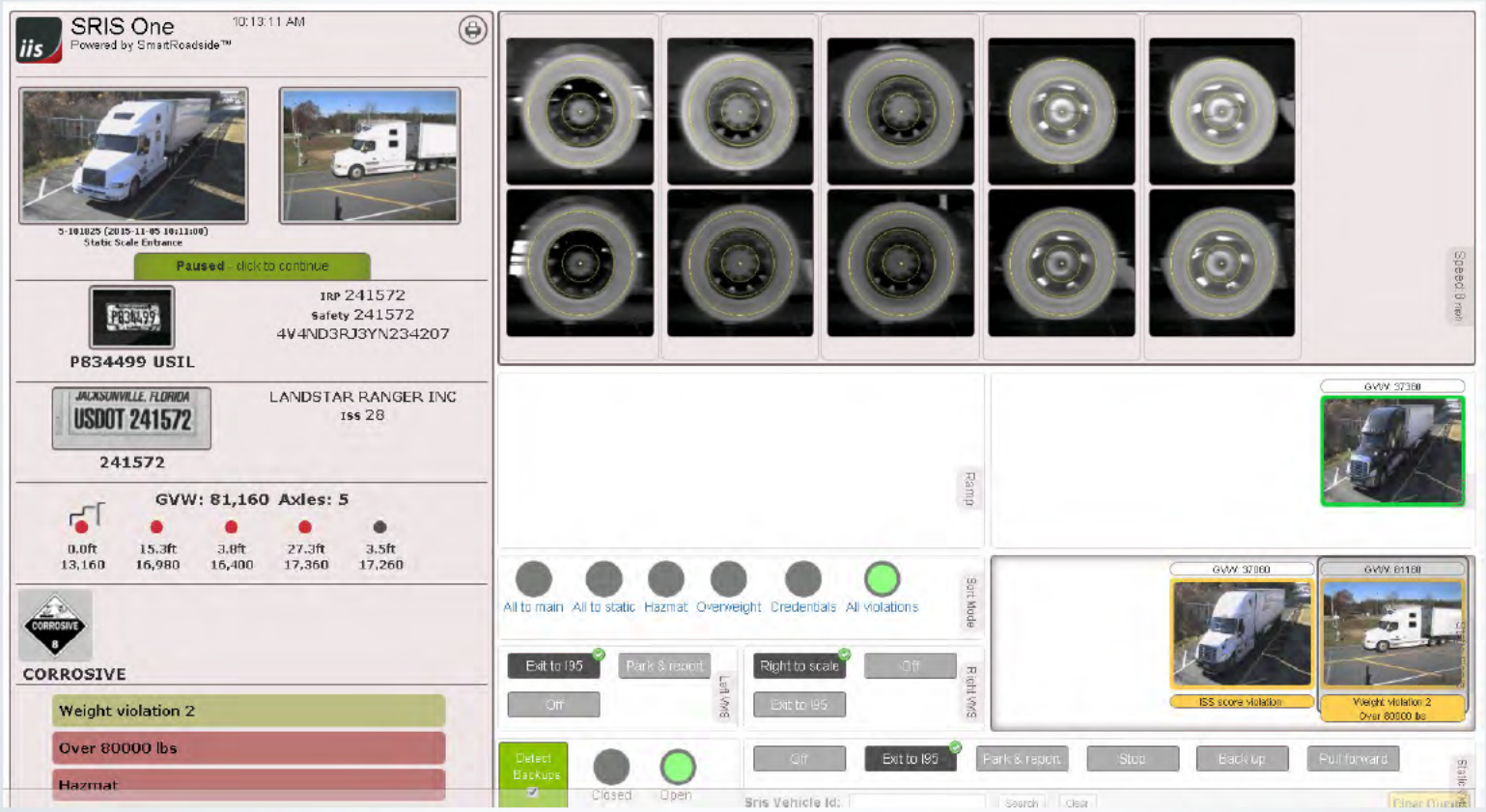
SRIS is the most comprehensive CVE solution in the market



- ✓ *Objective free-flow inspection systems that automatically identifying high-risk vehicles from the roadside.*
- ✓ *Solution that allows lead agencies to focus their resources more efficiently & effectively without interfering in the flow of commerce.*
- ✓ *Electronic screening that helps level the playing field in the trucking industry.*

Smart Roadside Screening (SW)

SRIS Single Interface



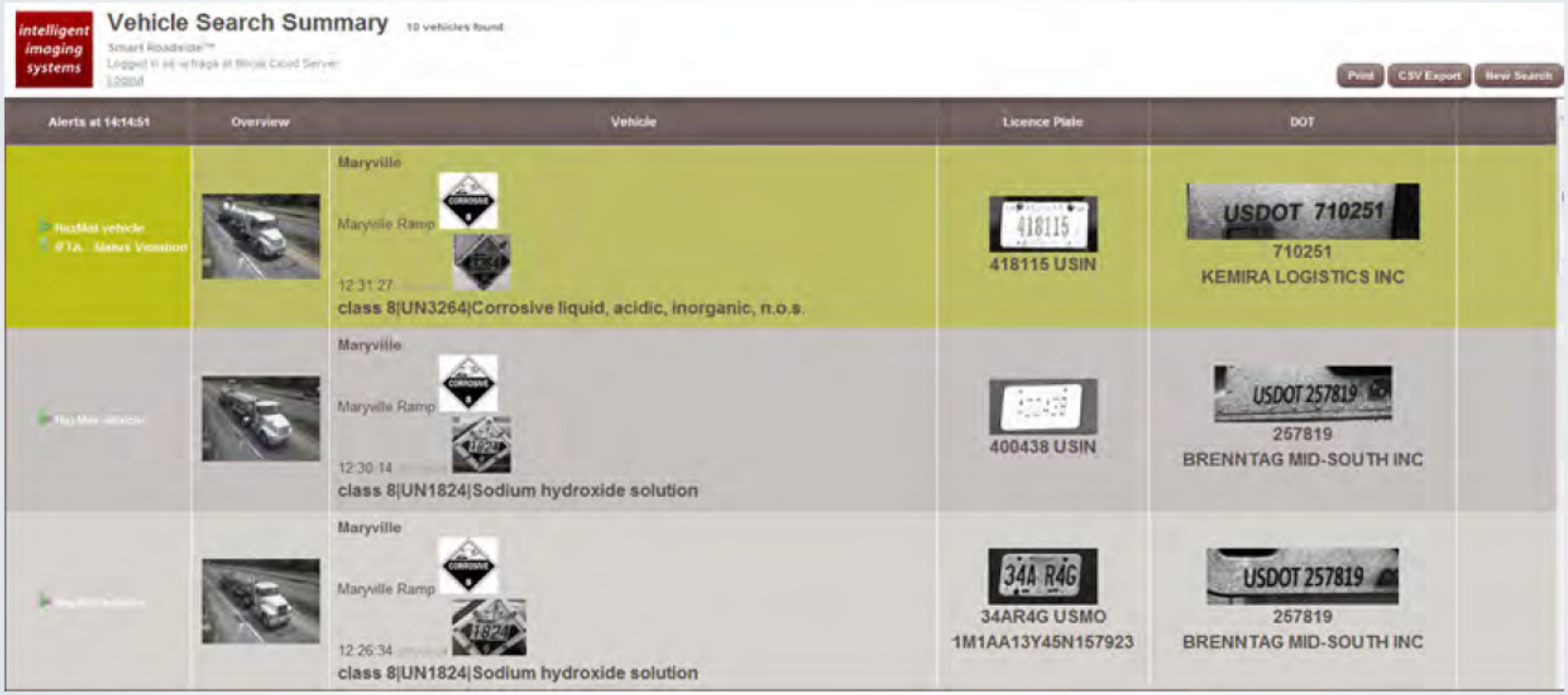
ALPR + AUNR (HW)

Two sensors are better than one

Accuracy of Identifying a Specific Truck using database cross reference and true validation algorithm	***94-98%***
Combined Accuracy at Ramp Speed (5-55mph)	96-98%
Combined Accuracy at High Speed (55-75mph)	94-96%

Hazardous Materials Placard Reader (HW)

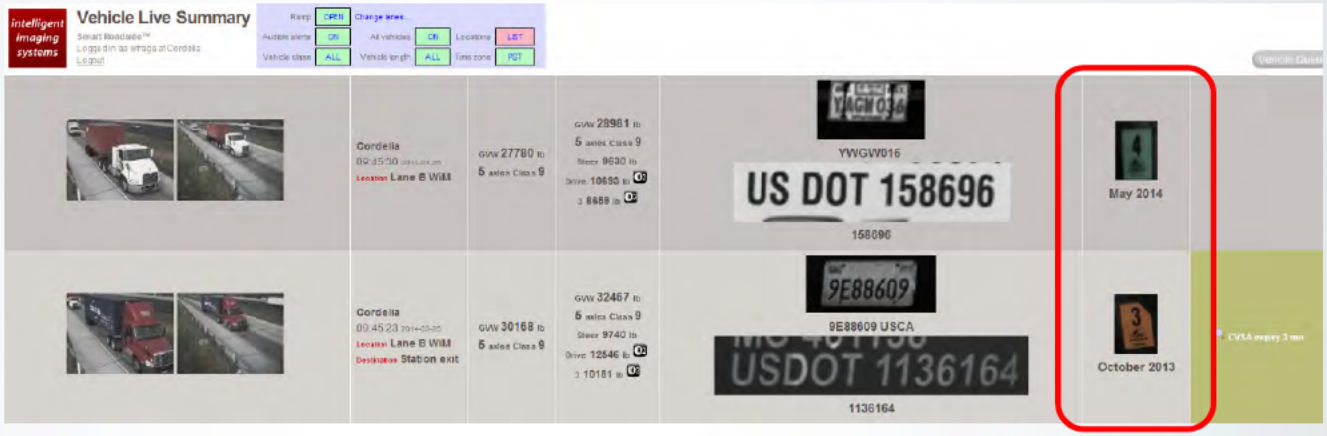
Software upgrade to Automated USDOT Reader

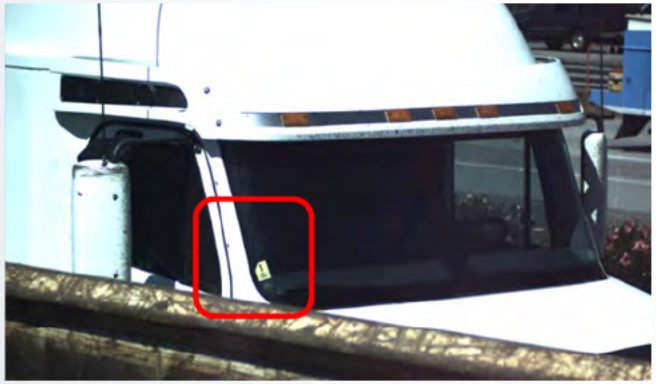


93%+ decode rates

CVSA Sticker Reader (HW)

Reads sticker issue year & calculates the expiry date



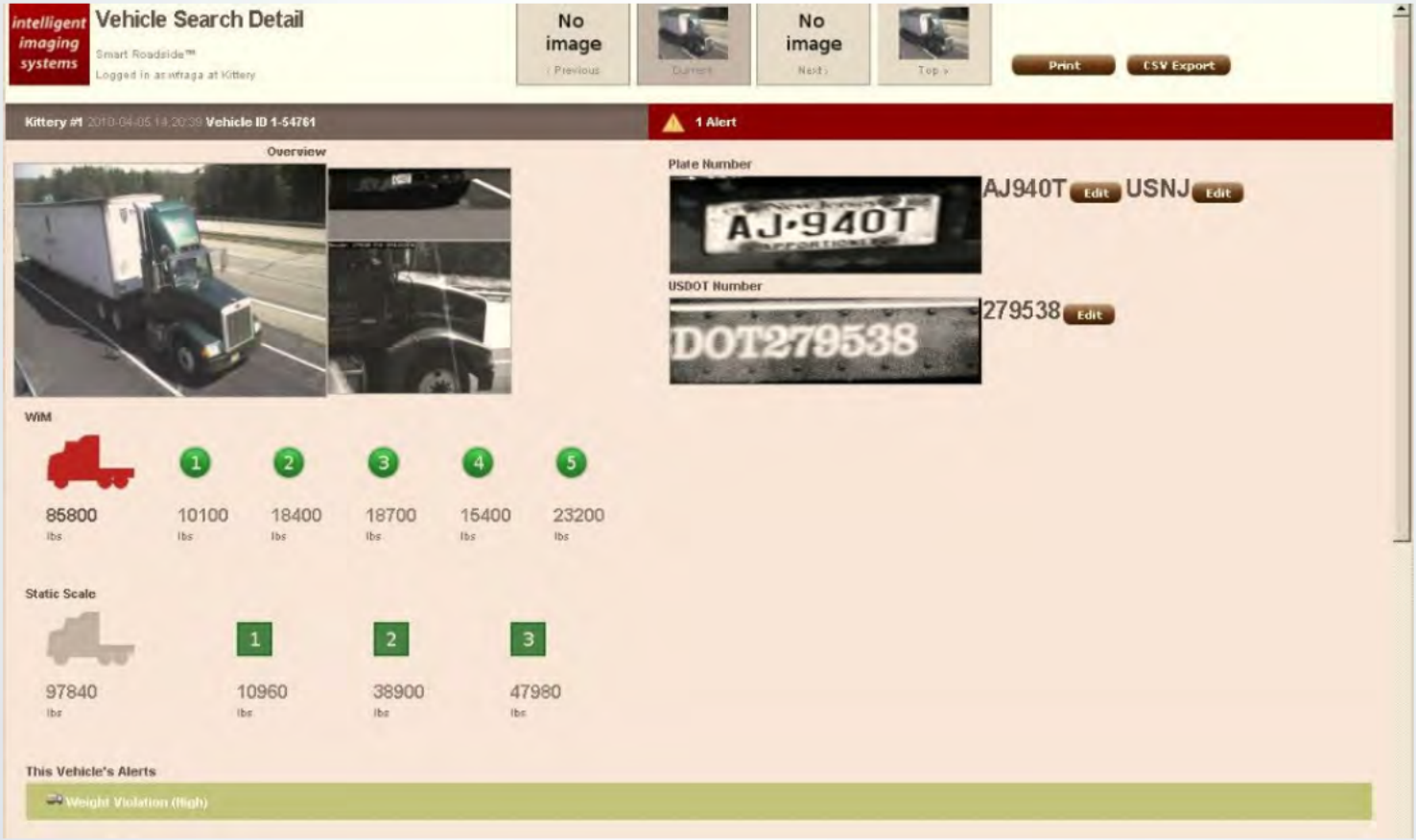




94%+ decode rates

Weight Systems (HW)

COTS Integration to all Static and WIM vendors

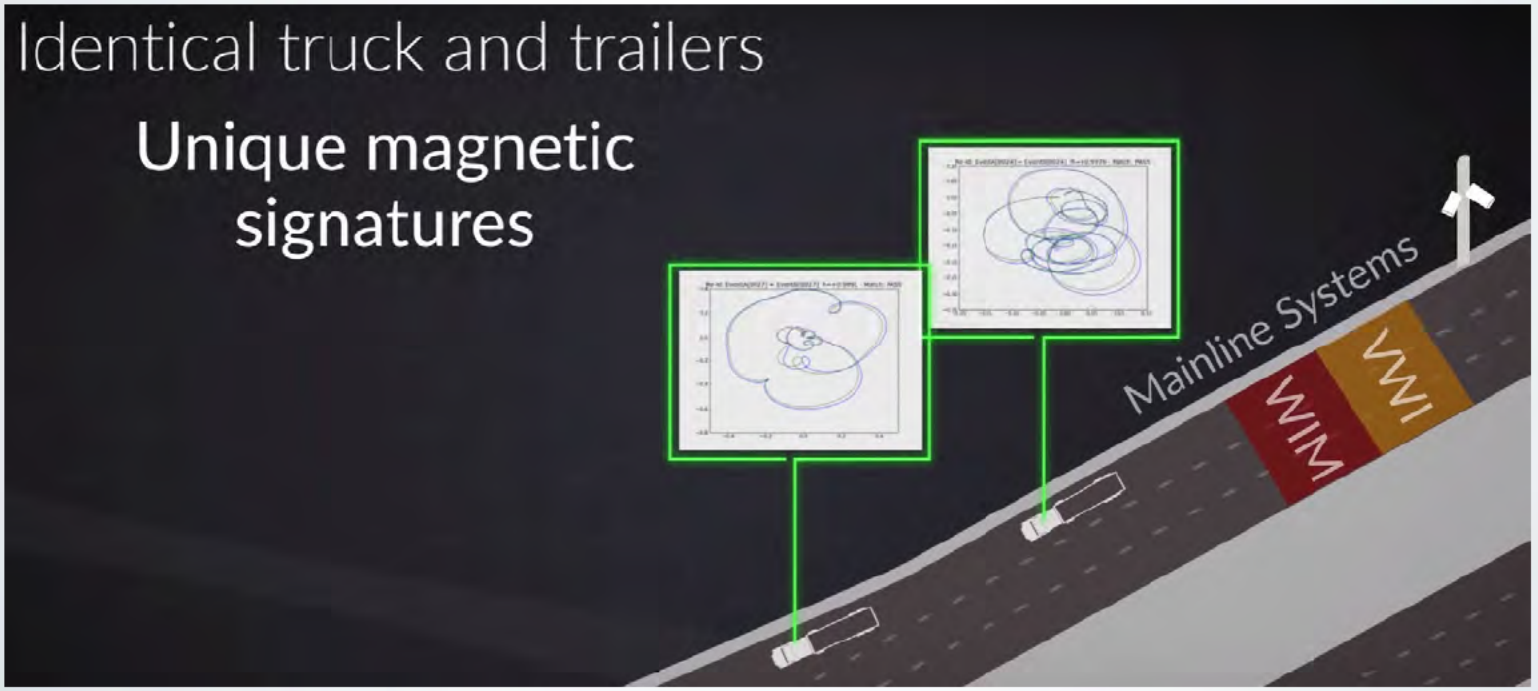


Vehicle Waveform Identification (HW)

Magnetic Fingerprint matching

http://intelligentimagingsystems.com/videos/

96%+ truck identification rates



Vehicle Waveform Identification (HW)

Magnetic Fingerprint matching
http://intelligentimagingsystems.com/videos/

- ✓ Screen & sort trucks on the mainline
- ✓ Eliminate redundant WIMs & sensors on the ramp
- ✓ Accurately track trucks for compliance

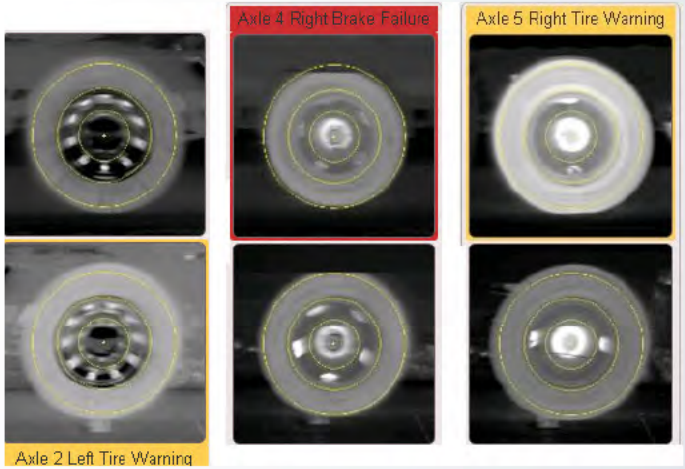


Automated Thermal Imaging (HW)

automatically screen a CMV's mechanical running gear

http://intelligentimagingsystems.com/videos/



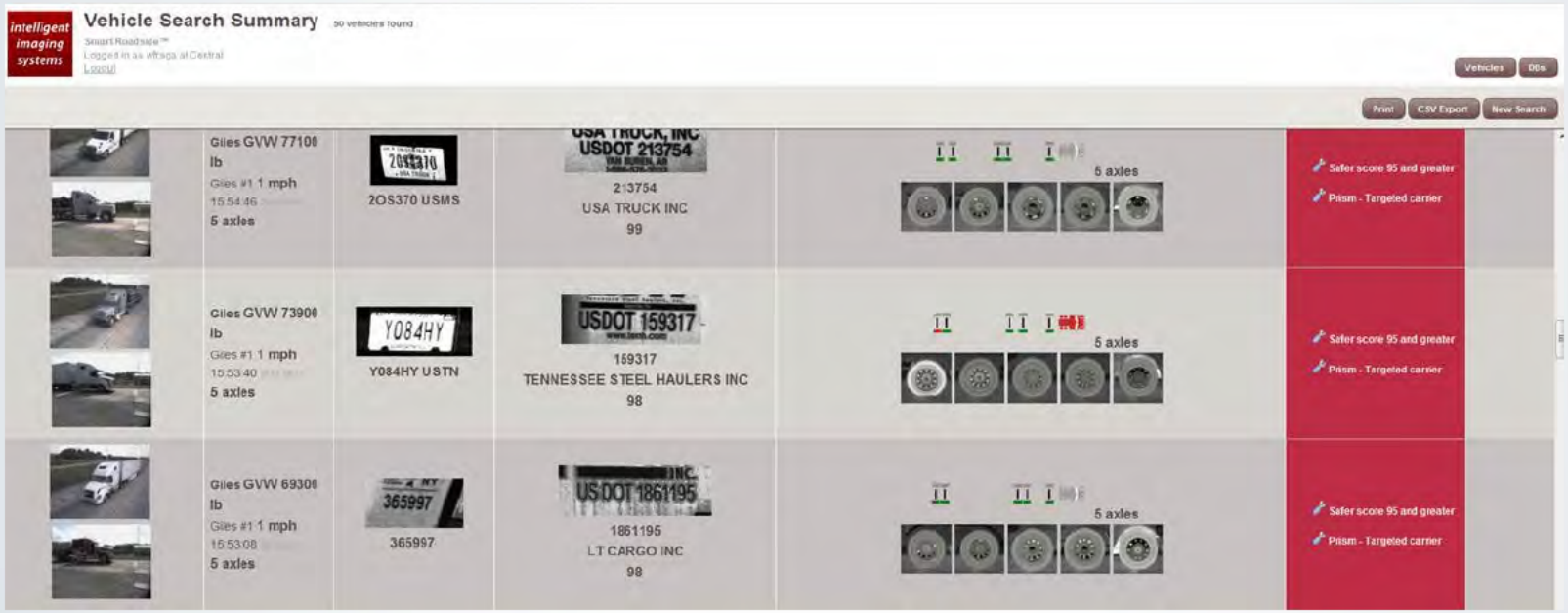


- ✓ identifying thermal anomalies such as wheel bearing failures, loose wheels, flat tires, and non-operational or out of adjustment brakes.

Automated Thermal Imaging (HW)

Integrated with other e-screening solutions

http://intelligentimagingsystems.com/videos/



Automated Thermal Imaging (HW)

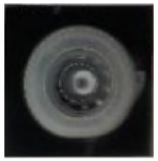
ATIS - Alberta

http://intelligentimagingsystems.com/videos/

90%+ detection rate for bad breaks & flat tires









Missing Studs

Blown Inside Tire

Tanker Recognition (HW & SW)

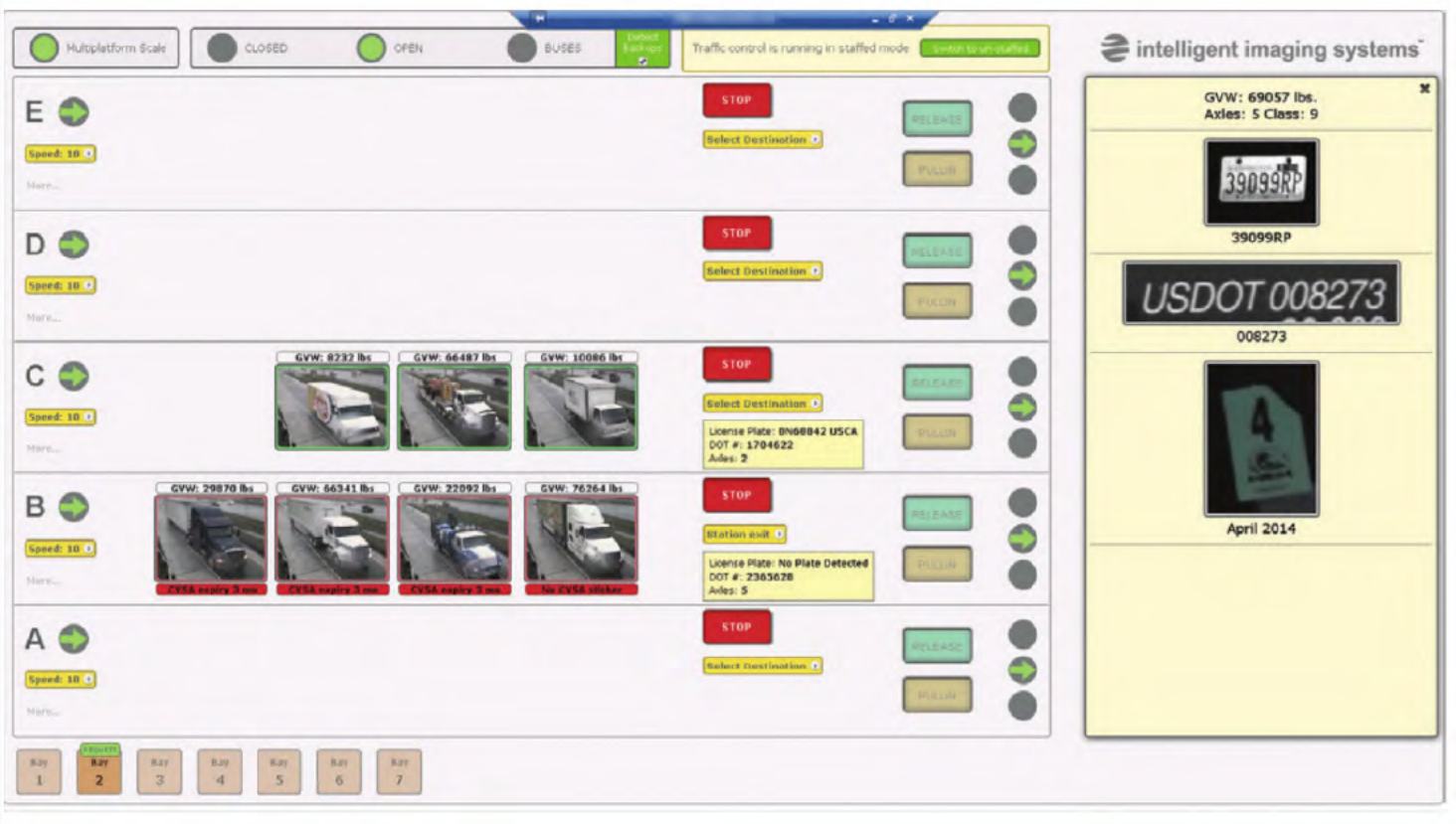
Text

- ✓ Automatically identify tanker trailers
- ✓ Utilize existing Overview Camera Systems
- ✓ 85% + performance
- ✓ Eventual general classification



Advance Lane Control (HW)

Facility Management



Mainline Screening & Messaging

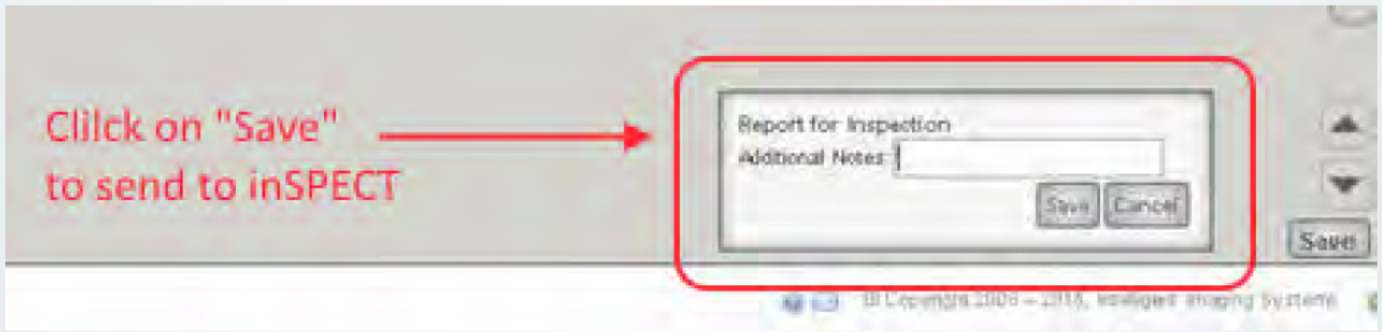
SRIS + VWI + VMS



Inspection Integration

Smart Roadside + Iteris inSPECT

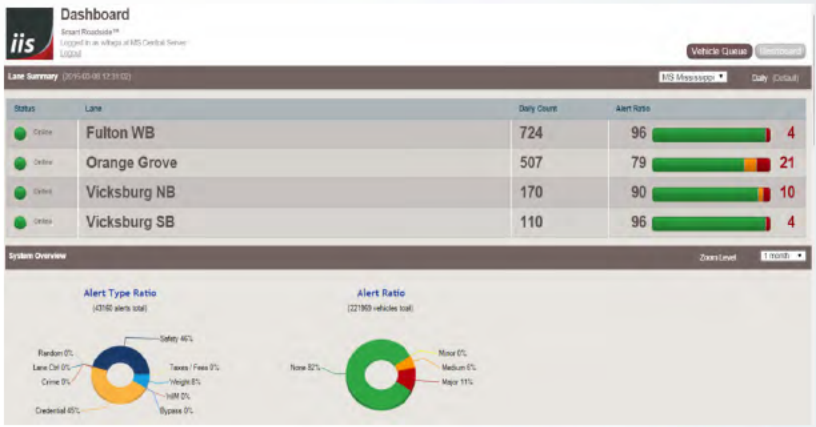




Reporting

Centralized Monitoring & Management Dashboards







Drivewyze Technologies

Drivewyze is **smart mobility services** company for the transportation industry

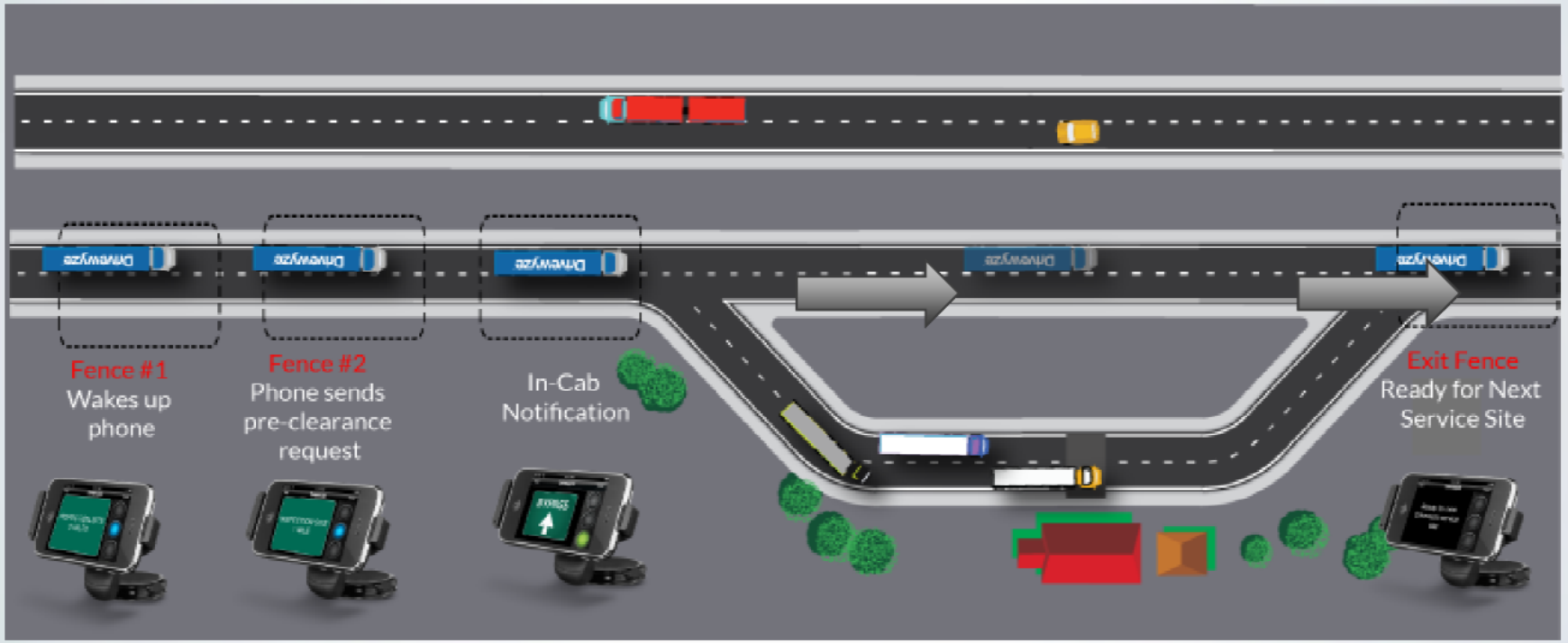
ELD Partners

Over 1M Trucks



Weigh Station Bypass

How Does It Work?



Weigh Station Bypass

Driver View

- ✓ Hands Free
- ✓ Visual & Audible alerts
- ✓ iOS, Android, ELDs



Weigh Station Bypass

Agency View

Drivewyze™
Powered by Smart Roadside™

Vehicle Search Summary 10 vehicles found

Smart Roadside™
Logged in as wfraga at Drivewyze.com
Logout

Vehicles | DBs

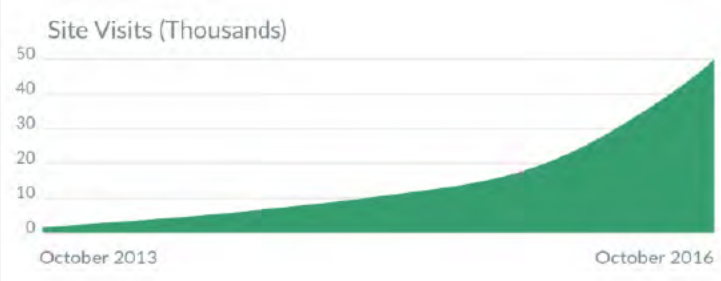
Print | CSV Export | New Search

Overview	Carrier	Vehicle	Driver	Clearance Result	Messages at 14:09:36	
	CT Danbury I-84 EB 14:00:46 2014-03-24 USDOT #80806 J B HUNT TRANSPORT INC	1HSDHSJR9CJ613498		Bypass		
	CT Waterford I-95 SB 07:38:52 2014-03-24 USDOT #929186 B L KITCHEN TRANSPORTATION LLC	71055 USMA		Bypass		
	CT Danbury I-84 EB 06:18:30 2014-03-24 USDOT #841776 X-TRUX INC	25764 USSD		Follow road signs	Credential Check	
	CT Middletown I-91 NB 04:48:01 2014-03-24 USDOT #80806 J B HUNT TRANSPORT INC	1FUJGBDV7ALAN6630		Bypass		

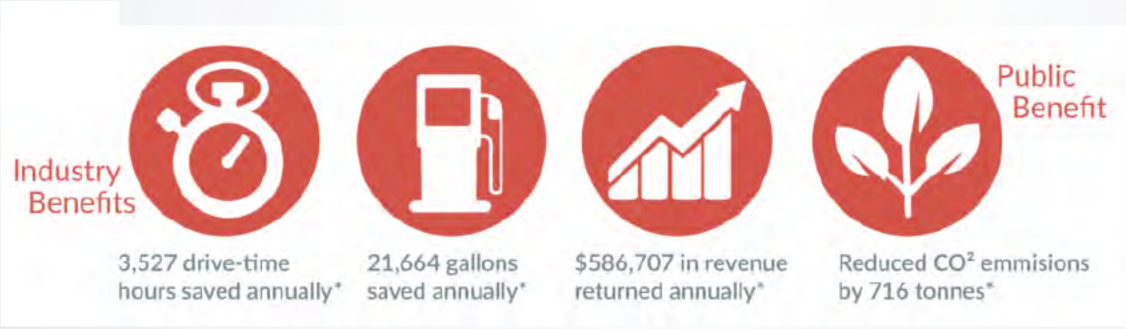
Weigh Station Bypass

Agency View









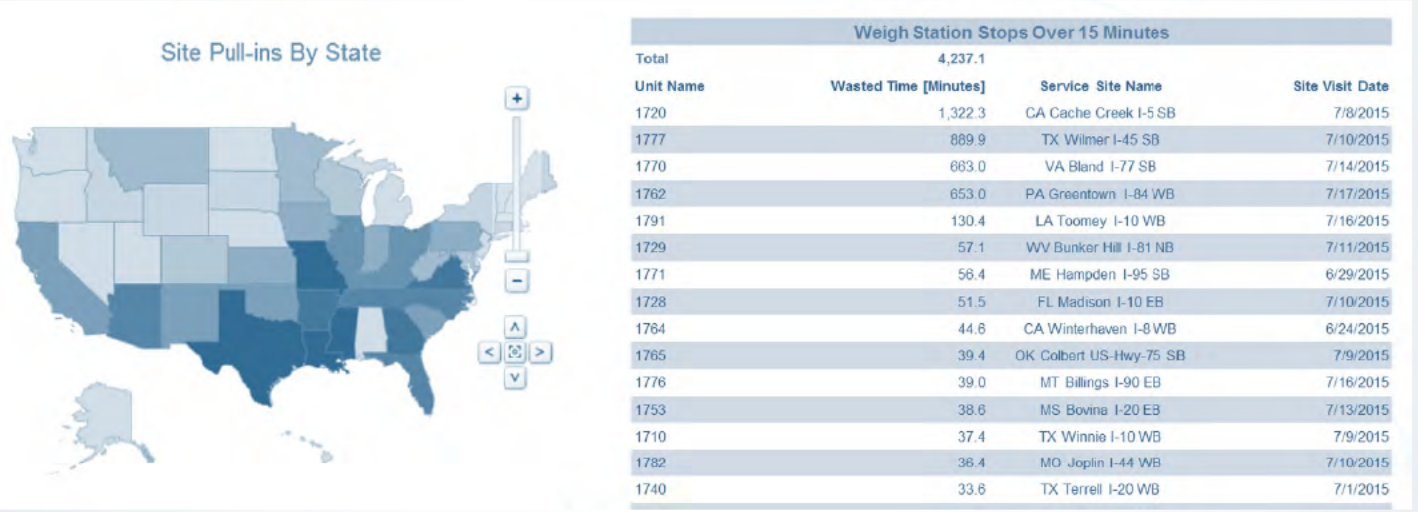
Weigh Station Bypass

Carrier Analytics



Weigh Station Bypass

Carrier Analytics



Weigh Station Stops Over 15 Minutes			
Total	4,237.1		
Unit Name	Wasted Time [Minutes]	Service Site Name	Site Visit Date
1720	1,322.3	CA Cache Creek I-5 SB	7/8/2015
1777	889.9	TX Wilmer I-45 SB	7/10/2015
1770	663.0	VA Bland I-77 SB	7/14/2015
1762	653.0	PA Greentown I-84 WB	7/17/2015
1791	130.4	LA Toomey I-10 WB	7/16/2015
1729	57.1	WV Bunker Hill I-81 NB	7/11/2015
1771	56.4	ME Hampden I-95 SB	6/29/2015
1728	51.5	FL Madison I-10 EB	7/10/2015
1764	44.6	CA Winterhaven I-8 WB	6/24/2015
1765	39.4	OK Colbert US-Hwy-75 SB	7/9/2015
1776	39.0	MT Billings I-90 EB	7/16/2015
1753	38.6	MS Bovina I-20 EB	7/13/2015
1710	37.4	TX Winnie I-10 WB	7/9/2015
1782	36.4	MO Joplin I-44 WB	7/10/2015
1740	33.6	TX Terrell I-20 WB	7/1/2015

96.3 hours time saved

638.4 gall. fuel saved

$14,778.96 dollars saved

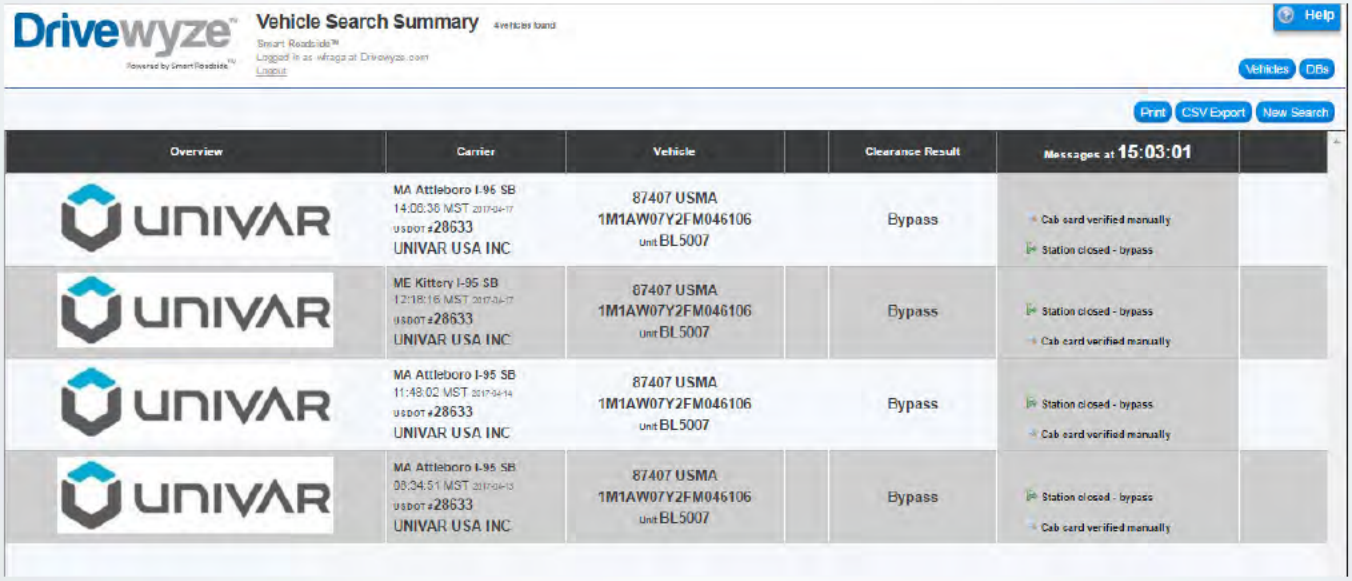
16.9 tonnes C02 reduced

Data Sharing

Pilot with CT, MA & ME

Goal: Reduce unnecessary inspections

Vehicle site activity is visible across state lines within Drivewyze Agency Portal

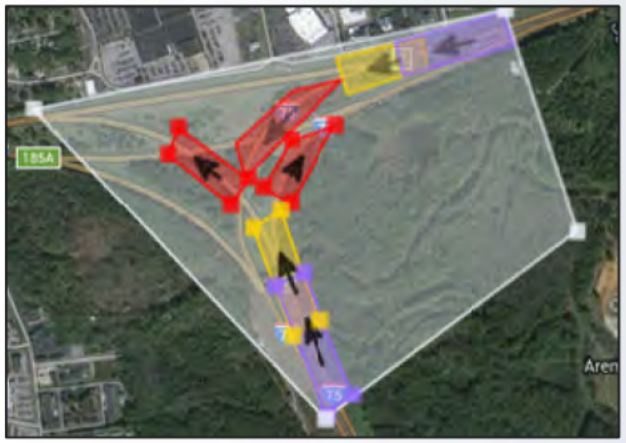


Driver Safety Notifications

Roll-Over Pilot

- ✓ 6 States, 37 sites & 15,000 trucks
- ✓ Sent drivers information describing new high rollover warning feature





- ✓ App produces warning notification of entering high rollover risk area

Roll-Over Notification Network

Results & Full Deployment

17% reduction	12% reduction	Launching Spring 2017
in incidences of excessive speed, despite existing road signage	in lateral forces acting on trucks through the curve	in 19 states – 100 sites

Talk to us about participating



Construction Zone Notifications

Concept

- Linkage to other Safety related data for trucks:
  - ✓ Work zone Alerts
  - ✓ Weather Alerts
  - ✓ Emergency Alerts
  - ✓ Any 511 message of interest
  - ✓ Applications by several partners underway



Truck Parking

Projects in MI, FL and OH

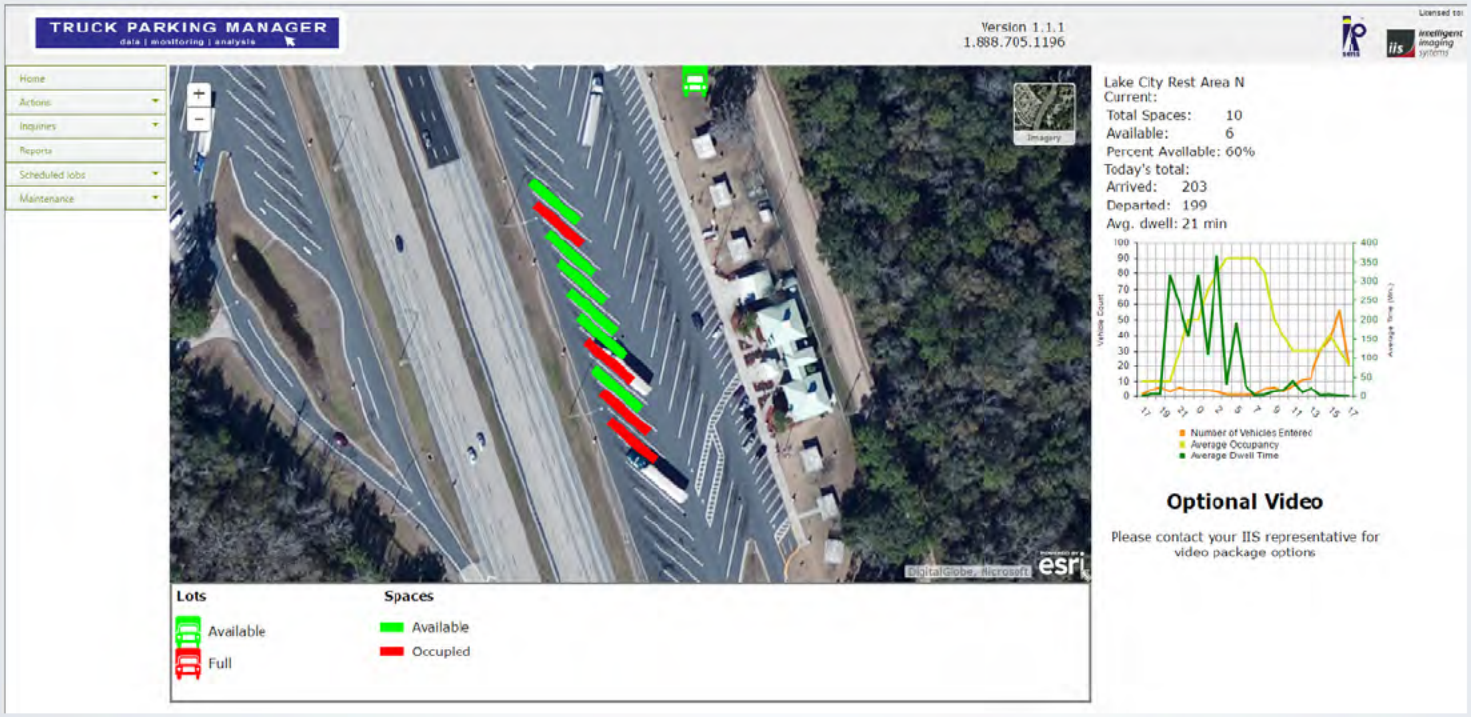
- ✓ FHWA reports > 83% of drivers take longer than 30 minutes to find parking
- ✓ Drivers who can't locate parking before reaching hours of service limits are often forced to park illegally or unsafely, on shoulders of highways, off-ramps, abandoned facilities
- ✓ Improve utilization of existing parking w turnkey solution:
  - Accurately Collect Data
  - Group, Process & Manage Data
  - Disseminate Information Timely



Truck Parking

Similar Constraints / Variables to CVE

- ✓ Fully developed, COTS software collects, analyzes info from sensors at all sites, compiles data.



Expedited Level III

Field Trial – MD, DE & VA

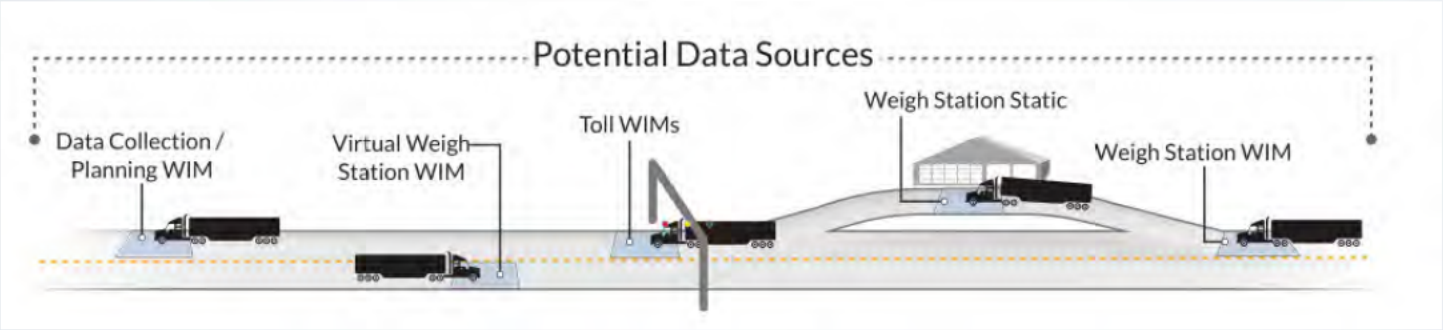
- ✓ In-motion wireless transfer of inspection data (truck + driver)
- ✓ Partial inspection automation (excl. seat belt + driver visual)
- ✓ Manual validation of inspection data by Agency LEO
- ✓ Level III inspection data processed 100% automatically

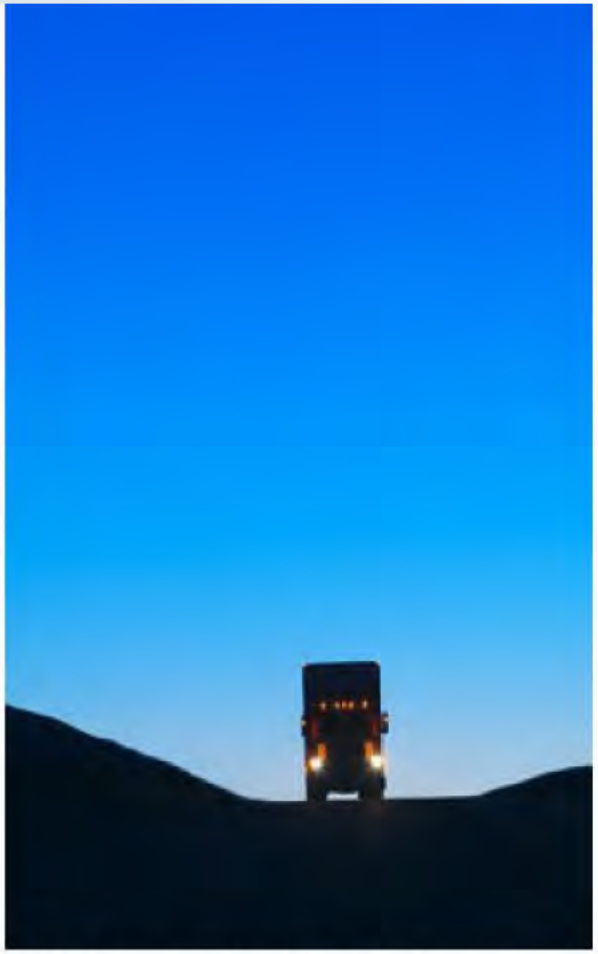


WIM Integration

Performance Based Weight Monitoring
http://intelligentimagingsystems.com/videos/

- ✓ Use one network of WIM for all DOT requirements
- ✓ Not limited by the co-location requirements of traditional DSRC Bypass
- ✓ Carrier & Vehicle weigh history
- ✓ Centralized WIM virtual calibration & error detection
- ✓ Monitoring strategic corridors & freight commodity flows





Is This a High-Risk Carrier?

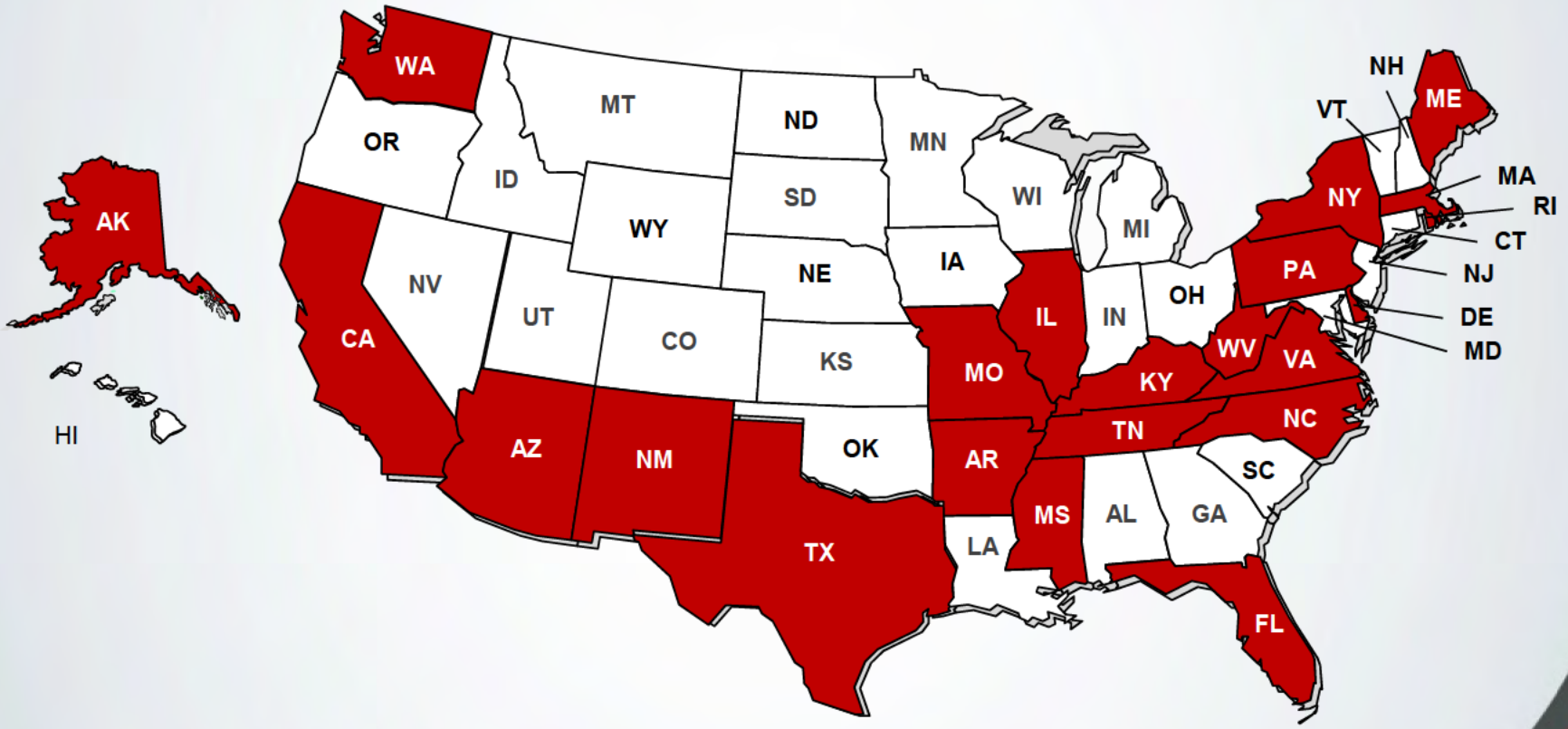
Thank You!

Enrique Cramer
Business Development Director
(778) 384-4341
ecramer@intelligentimagingsystems.com

Appendix

Smart Roadside Deployments

Operational in more than 100 sites in over 20 states



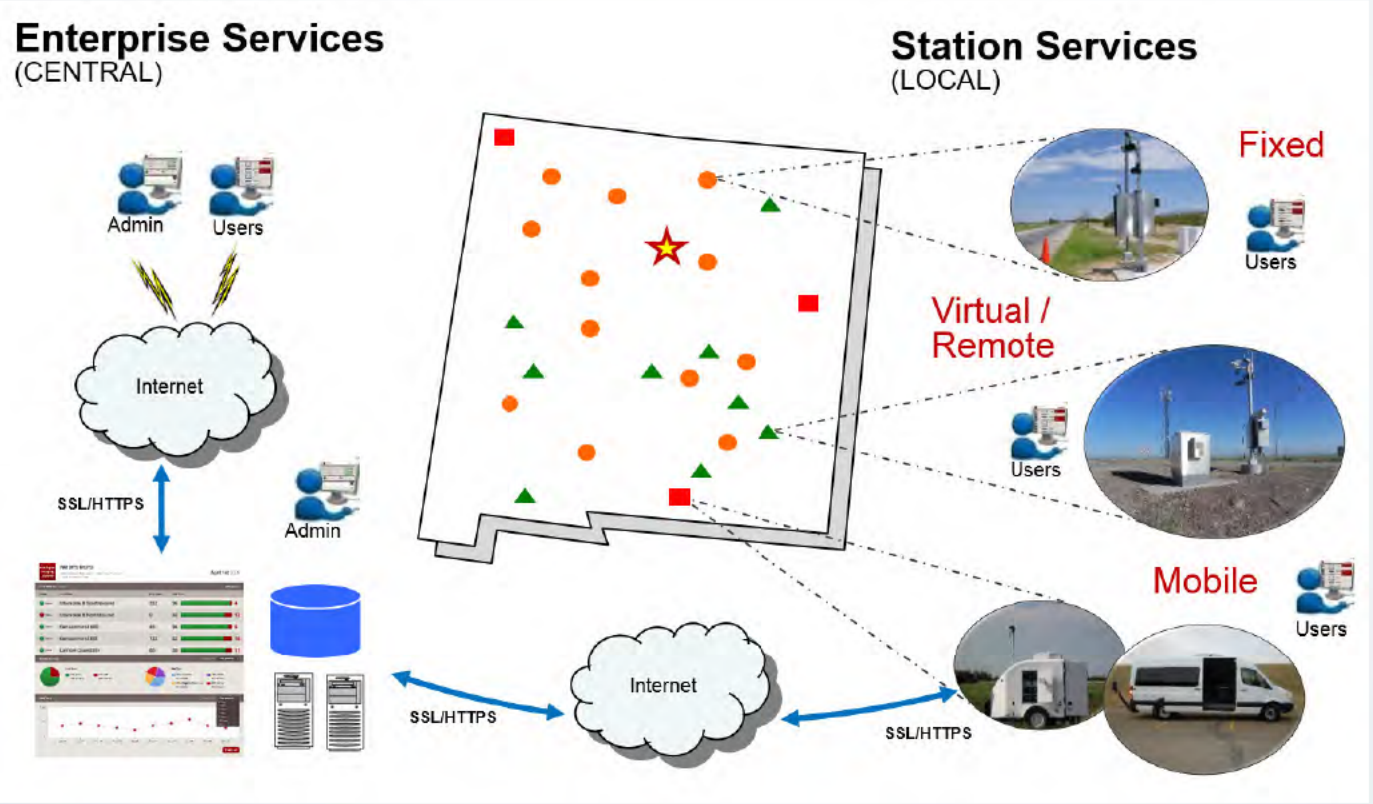
intelligent imaging systems

iis

Smart Roadside Screening (SW)

SRIS Hub & Spoke Architecture

✓ Cloud hosting & processing



Smart Roadside Screening (SW)

SRIS Data Integration & Control

- ✓ 100% transparency into the source of all data utilized
- ✓ Data is known, auditable and verifiable
- ✓ Utilizes authentic authoritative data sources: State CVIEW, SAFER, PRISM, NCIC, IFTA, IRP, CDLIS, DEA, DHS, Permitting, Hot Lists
- ✓ Direct Access to authoritative, auditable source data, through NLETS

Automatic License Plate Reader (HW)

Higher read rates at highway speed than any other solution

Typical ALPR Accuracy as Stand Alone *Sub-System*	**80-90%**
ALPR Accuracy at Ramp Speed (5-55mph)	85-90%
ALPR Accuracy at High Speed (55-75mph)	80-85%
ALPR out-of-state jurisdiction cross-match accuracy	99%

Automatic USDOT Number Reader (HW)

Higher read rates at highway speed than any other solution

Typical AUR Accuracy as Stand Alone Sub System	*70-90%*
AUR Accuracy at Ramp Speed (5-55mph)	75-90%
AUR Accuracy at High Speed (55-75mph)	70-80%

Automated Thermal Imaging (HW)

ATIS complimentary to Performance Based Break Testers

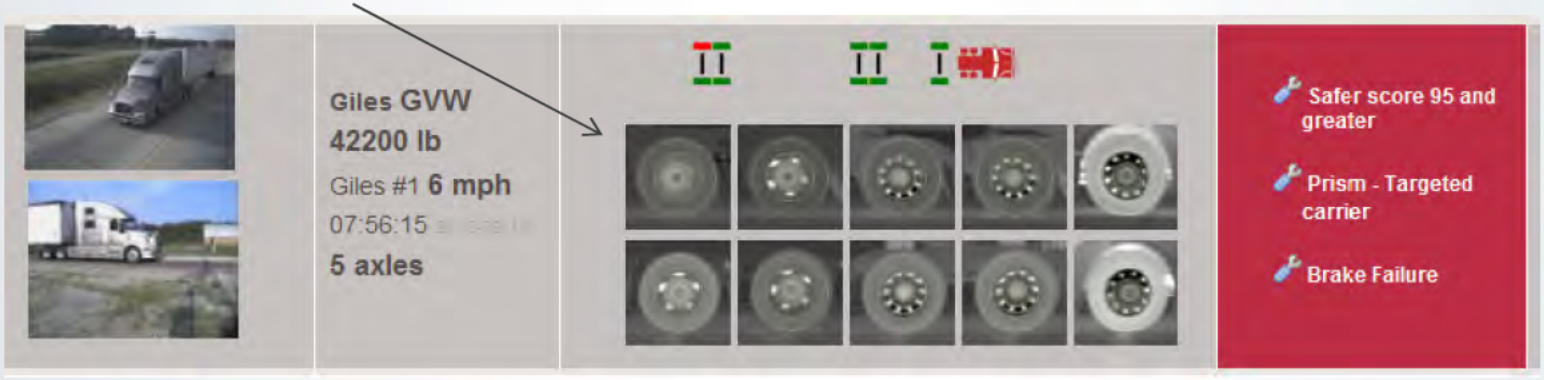
	ATIS Screening	PBBT Diagnostic
Capabilities		
Identifies non-working brakes	✓	✓
Works at speed as an unmanned screening tool (free flow)	✓	X
Identifies the causes of non-working brakes	X	✓
Identifies other mechanical issues (i.e. flat tires, missing studs, etc.)	✓	X
Measures axle weights	X	✓
Time to identify non-working brakes	seconds	minutes
Uses		
High Volume Free-Flow Traffic	✓	X
Set criteria to place a vehicle out-of-service	X	✓
Used at fixed facilities	✓	✓
Used as mobile units[1]	Manual IRIS	✓
Price range	$$$	$$

Automated Thermal Imaging (HW)

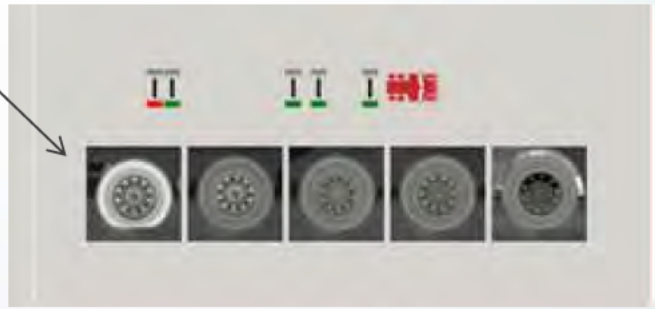
ATIS – Tennessee (Giles)

http://intelligentimagingsystems.com/videos/

Brake Failure= 22,000 Trucks (2% of total traffic)



Tire Failure = 8,500 Trucks (1.3% of traffic)



Deployment Configurations

Fixed (Mainline & Ramp), Virtual (Remote & unmanned), & Mobile (Van & Trailer)











Proven Results

Lordsburg POE, NM



Sample of benefits at one weigh station before and after screening solution:

	2009	2012
Total Inspections	14,713	12,001
OOS Rate	37.60%	67.38%

State Partner Recognition

Smart Roadside Awards

Roadway Safety Foundation

U.S. Department of Transportation
Federal Highway Administration

2011 Winner Program Planning, Development and Evaluation Category

ITS AMERICA

2009 Winner Best New Innovative Products or Services

2010 Winner Best New Innovative Products or Services

2011 Finalist Best New Innovative Products or Services

2014 Winner Best New Innovative Products or Services

California Transportation Foundation
CTF

2014 Winner Safety Project of the Year

ITS ▪ STI CANADA

2010 Winner ITS' Provincial/ Federal Category

2012 Winner ITS' Provincial/ Federal Category

HARVARD Kennedy School
ASH CENTER
for Democratic Governance and Innovation

2013 "Top 5" Innovations in American Government

GHSA
Governors Highway Safety Association
The States' Voice on Highway Safety

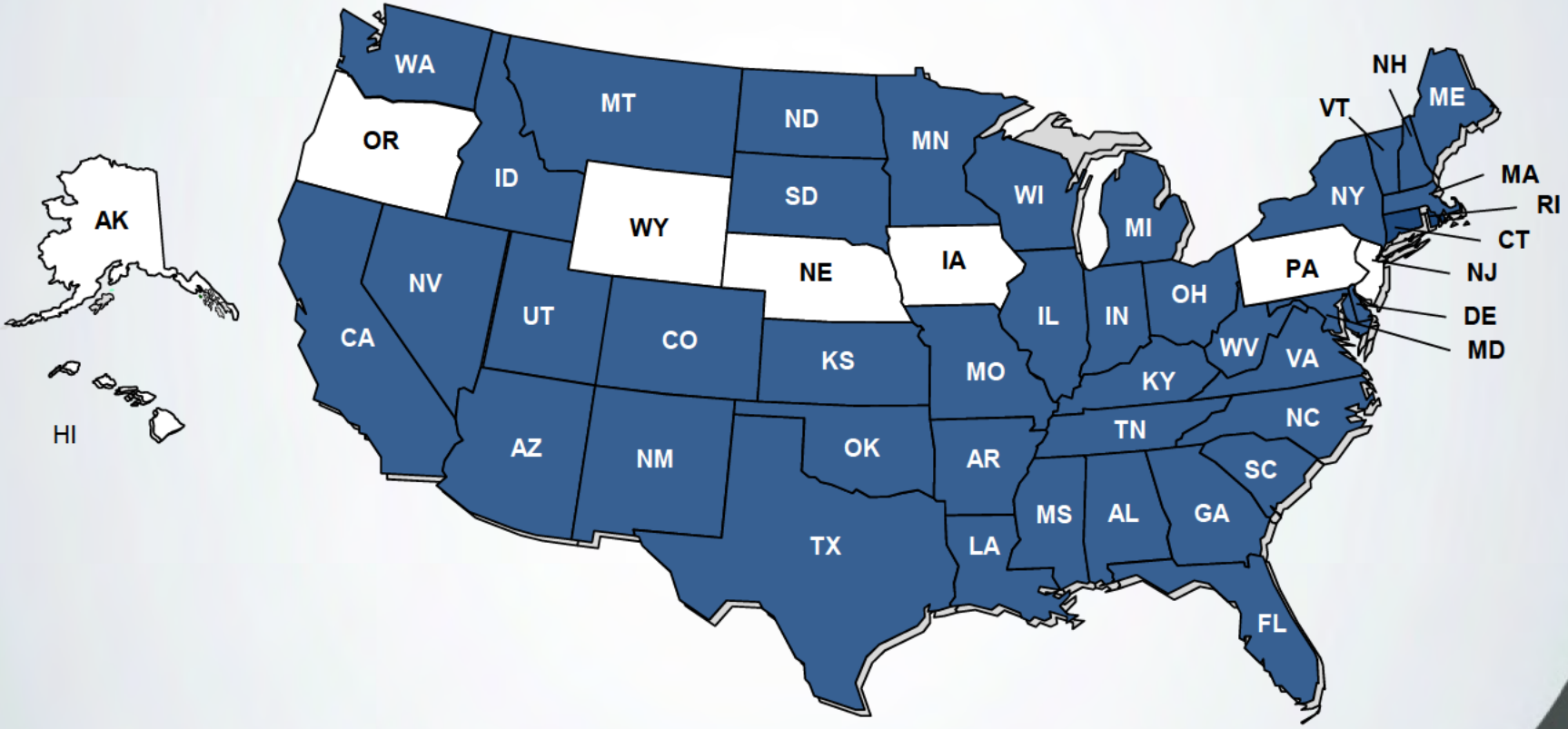
2012 Winner Government Highway Safety Association Peter K. O'Rourke Special Achievement Award

ITS-NY
Intelligent Transportation Society of New York

2009 Winner Innovative Practice Category

Weigh Station Bypass Network

47 agencies, 42 states, 1 province, over 600 sites



CASE – CVISN E-SCREENING AND OVERWEIGHT SCREENING PROJECT

STUDY COMMITTEE MEETING: May 24, 2017

Project Overview

Goal

Implementation document for a virtual electronic screening and weigh-in-motion pilot project jointly supported by CTDOT and CTDMV

Project Overview

Objectives

- Define Preferred Roadway Segment for each Priority Corridor
- Conduct Feasibility Analysis on Preferred Roadway Segments to determine type of facility/technology
- Review most appropriate functionalities and technologies
- Pros/cons from other states that currently use the technologies identified
- List of technological components and data modules
- Estimated costs of equipment and installation
- Estimated future maintenance costs
- Evaluation of bypass potential for each preferred roadway segment
- Prioritize order of site installations
- List of steps for implementation/timeline

Project Overview

Out of Scope

- Support for development of a multi-agency, statewide CT Commercial Vehicle Program mission and goals statement and evaluative/performance metrics
- Modeling the process for multi-agency oversight and joint decision-making for CT's Commercial Vehicle Enforcement Program
- Multi-Agency Commissioner Briefing
- Research on process and outcomes related to Commercial Vehicle citations/fines and fines paid

Project Plan and Progress to Date

Study Committee Meetings

- **December 21, 2016**
  - ✓ Research Team Work Plan Overview
  - ✓ Florida Site Visit Overview
  - ✓ CTDOT Intelligent Transportation Systems Engineering
  - ✓ Vendor Overview: Mettler Toledo
- **January 25, 2017**
  - ✓ UConn Crash Repository
  - ✓ MaineDOT Commercial Vehicle Enforcement Program
  - ✓ Kentucky Automated Truck Screening System
  - ✓ Multi-Agency Commissioner Briefing Overview
- **February 22, 2017**
  - ✓ Research Team Work Plan Update
  - ✓ FHWA Truck Size & Weight Enforcement Technologies
  - ✓ MassDOT Commercial Vehicle Enforcement Program
  - ✓ Productivity Apex: Automated Enforcement in the ITS Environment

Project Plan and Progress to Date

Study Committee Meetings

- **March 15, 2017**
  - ✓ Research Team Work Plan Update: Feasibility Analysis
  - ✓ NYSDOT Commercial Vehicle Enforcement Program
  - ✓ Vendor Overview: IRD
- **April 26, 2017**
  - ✓ Research Team Work Plan Update: Appropriate Functionalities and Technologies
  - ✓ Research Team Work Plan Update: DRAFT Overview of Potential VSF Sites
  - ✓ Vendor Overview: Iteris
  - ✓ Discussion/Decision Items:
    - ➢ Quartz Piezo v. Single Load WIM

Project Plan and Progress to Date

Additional Activities

Meetings

- ✓ **Project Staff Meetings: 19 meetings facilitated by CASE, beginning October 28, 2017**
- ✓ **Connecticut Statewide Intelligent Technology System Project Meeting: December 20, 2017**
- ✓ **Multi-Agency Commissioner's Briefing: January 18, 2017**
- ✓ **CTDOT CT Freight Meeting: March 8, 2017**
- ✓ **Multi-Agency Evaluative/ Performance Metrics Meeting: May 5, 2017**

Project Plan and Progress to Date

Additional Activities *(cont.)*

CTDOT Interviews

- ✓Brad Overturf, Planning WIMs
- ✓John Korte, Highway Operations and Fiber Optics
- ✓Ed Block, Performance Measures and Pavement Deterioration
- ✓Don Braman, Oversize and Overweight Permits
- ✓Dave Hiscox, Bridge Maintenance

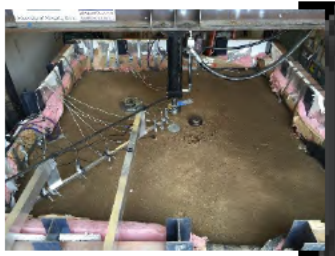
Project Plan and Progress to Date

Additional Activities *(cont.)*

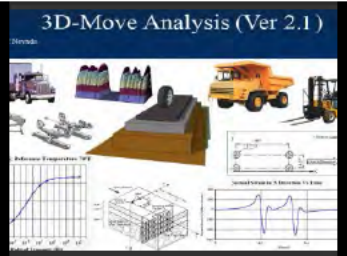
- **Site Visits**
  - ✓ **Florida Commercial Vehicle Enforcement: September 26 – 28, 2016**
  - ✓ **Connecticut Weigh Stations: February 21 – 23, 2017**
- **Observations**
  - ✓ **CTDMV Commercial Vehicle Enforcement Ride-Along: January 6, 2017**
  - ✓ **Massachusetts Commercial Vehicle Program PRISM Trailer: January 13, 2017**

Agenda and Objective Today

- **Discussion/Decision Items from Last Meeting**
  - ✓ **Update on Single Load v. Quartz Piezo WIM**
- **Presentations**
  - ✓ **Vendor: Intelligent Imaging**
  - ✓ **CTDOT: Planning WIMs**
  - ✓ **University of Nevada: Impact of Heavy Vehicles on Pavement**
- **Discussion/Decision Items**









IMPACT OF HEAVY VEHCILES ON FLEXIBLE PAVEMENTS

Principal Investigator: Elie Y. Hajj
Co- Principal Investigator: Raj V. Siddharthan

Pavement Engineering & Science Program
University of Nevada, Reno

May 24, 2017
Connecticut Academy of Science and Engineering (CASE)

Acknowledgments

- Nevada Department of Transportation (NDOT) P609-13-803
  - Mechanistic-Based Pavement Damage and Associated Cost from Oversize and Overweight (OS/OW) Vehicles in Nevada

- Federal Highway Administration (FHWA) DTFH61-13-C-00014
  - Analysis Procedures for Evaluating Superheavy Load Movement on Flexible Pavements

The contents reflect the views of the authors and do not necessarily reflect the official views and policies of the sponsors

Acknowledgments

- UNR Research Team
  - Research Associate Professor
    - Sherif Elfass

- Graduate Research Assistants
  - Dario Batioja
  - Farzan Kazemi
  - Hadi Nabizadeh
  - Mohamed Nimeri

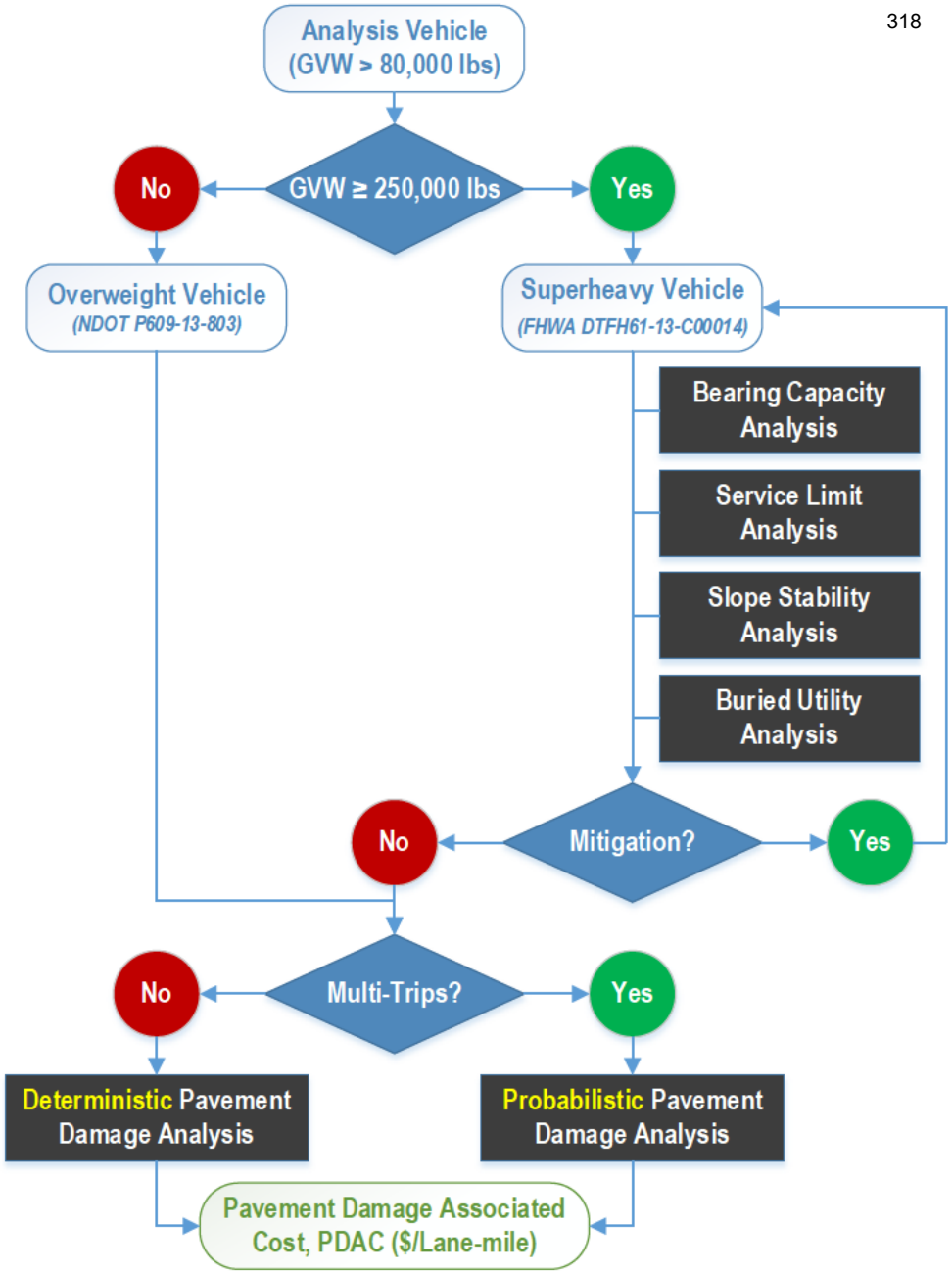
Overall Analysis Flowchart

Objectives:

- Assess the impact of heavy vehicles on flexible pavements.
- Develop a methodology for quantifying pavement damage and associated pavement damage costs.

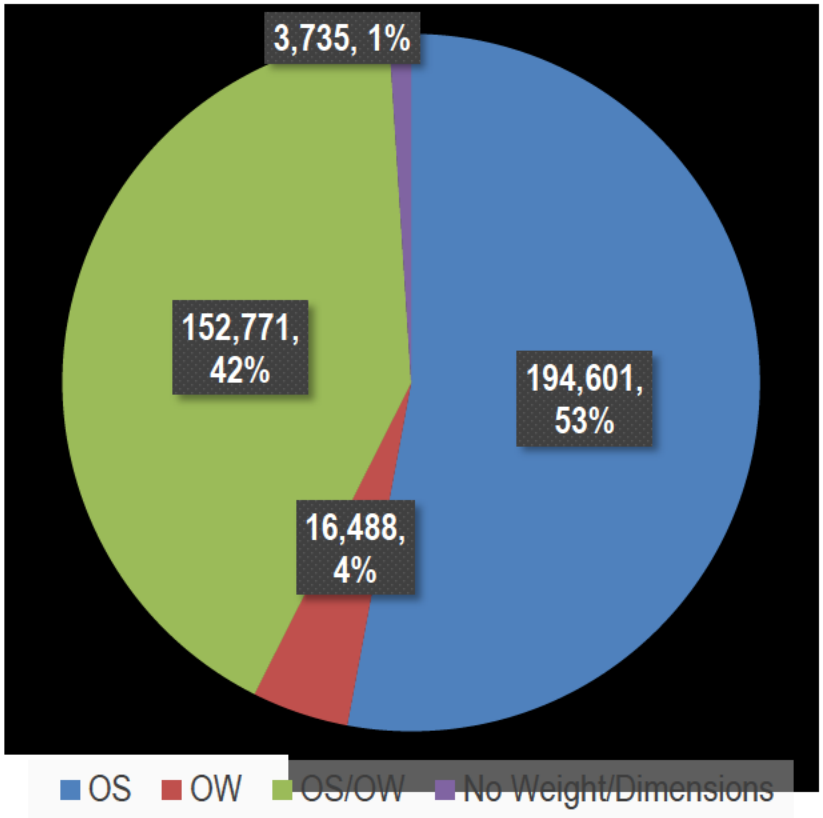
Overweight vehicle is defined based on Gross Vehicle Weight (GVW) > 80,000 lbs.

Superheavy load vehicle is defined based on GVW > 250,000 lbs.

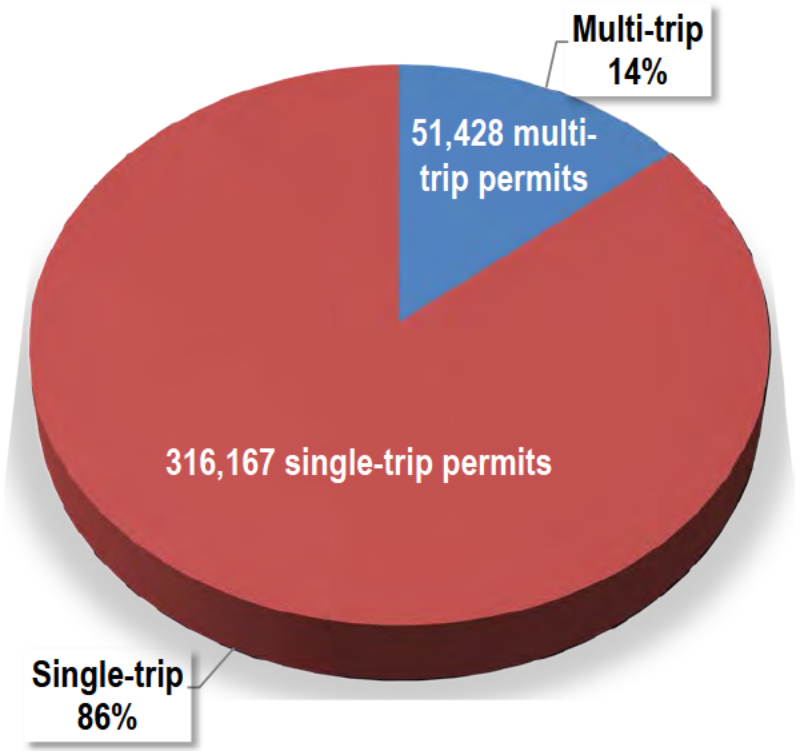


Nevada DOT Permits History (2004-2013)

Total Permits: 367,595



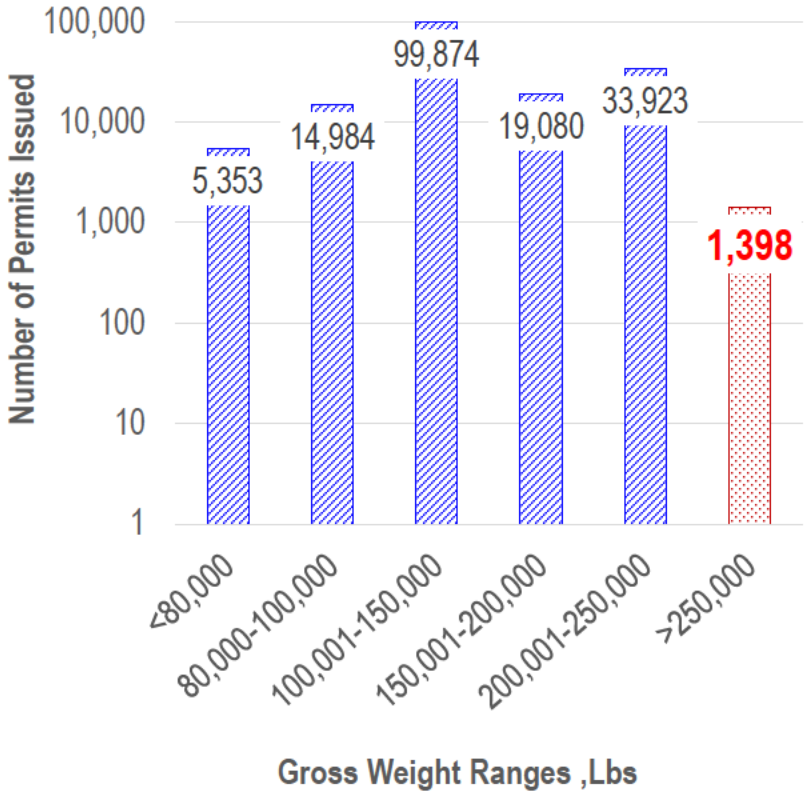
Single vs. Multi-trips



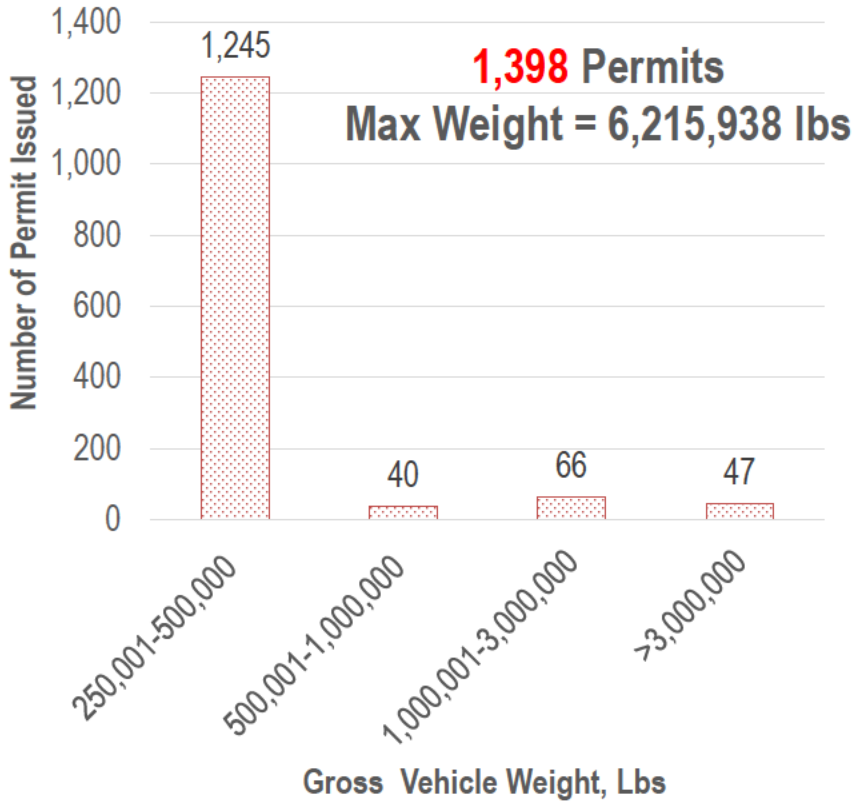
Multi-trips (annual/semi-annual): Vehicle operates without restriction during the permit duration

Nevada DOT Permits History (2004-2013) (Cont'd)

Distribution by GVW

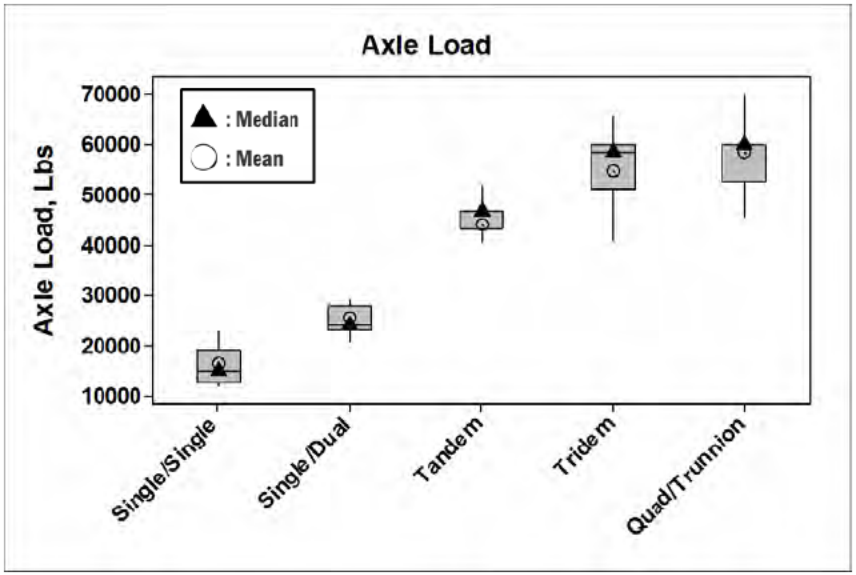


Superheavy Loads Permits

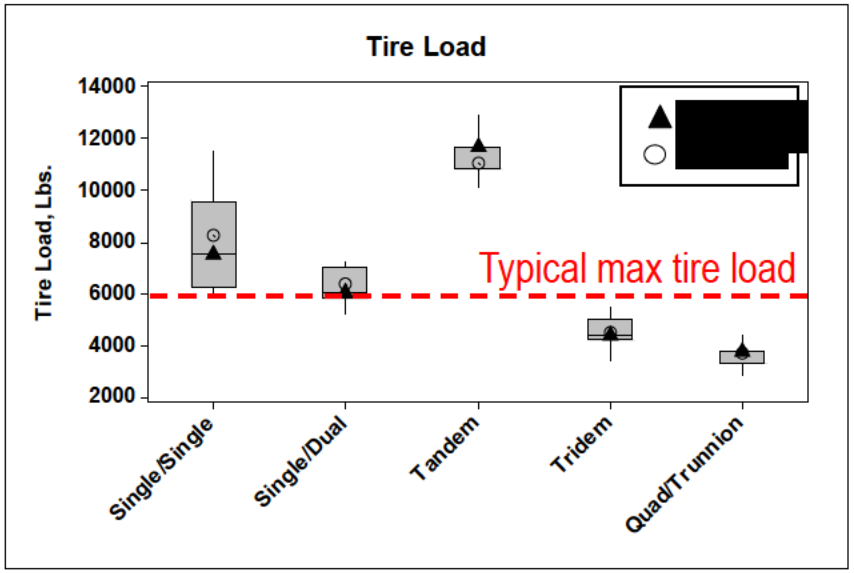


Nevada DOT Permits History (2004-2013) (Cont'd)

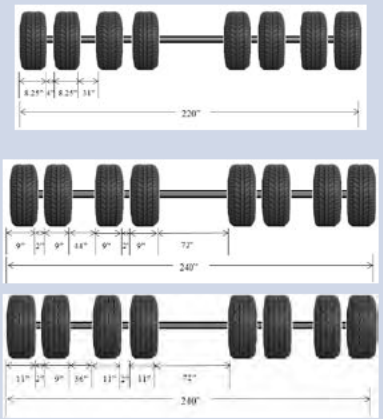
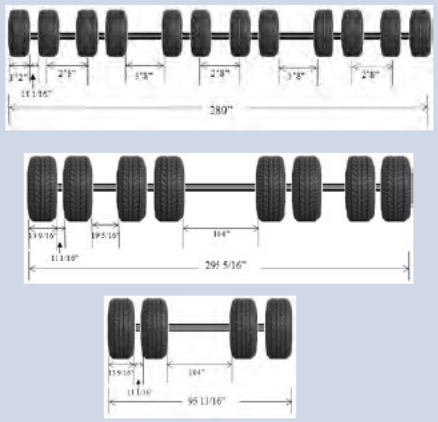
Axle Load Distribution



Tire Load Distribution

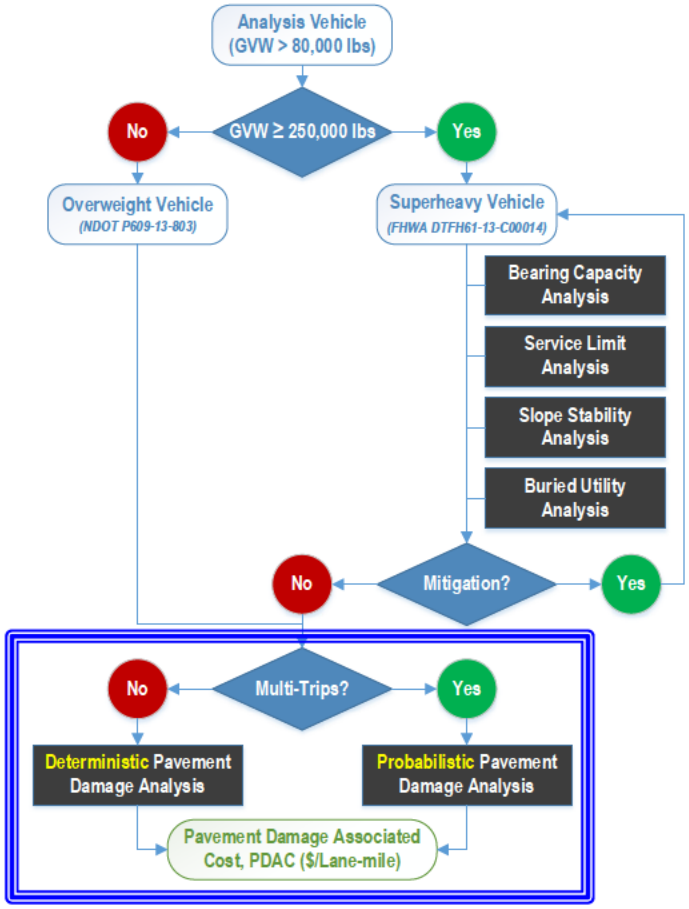


SHL Types and Axle Configurations
Samples Based on Review of Select Permits

SHL information for Select Permits	State Highway Agency		
	ARIZONA	LOUISIANA	NEW YORK
GVW (lbs)	647,855 - 1,180,000	402,240 - 3,660,551	200,000 – 855,000
Weight per Axle (lbs)	46,305 - 51,687	25,639 - 130,734	28,300 - 52,600
Number of tires/axle	8	4, 8, 12	4, 8
Axle width	18'4" - 20'4"	17'5" - 24'7 5/16"	12'10" - 13'6"
Center-to-center distance between adjacent axles	6'0" - 12'1"	4'7" - 11'3/4"	4'11" - 5'
Tire load (lbs)	5,000 - 6,460	7,028 - 16,341	3,538 - 6,575
Tire width	8 1/4" to 11"	1'1/2" - 1'2"	1'1/2" - 1'2"
Tire configuration/axle			NA

Impact of Heavy Vehicles of Flexible Pavements

PAVEMENT DAMAGE ASSOCIATED COST



Cost Allocation Methodology

Revised from Tirado et al. (2010)[1] approach to include Remaining Service Life (RSL)

- Comparison of pavement damage under heavy analysis truck relative to damage under select standard truck (e.g. 18-wheel truck).
  - *Requires calculation of pavement responses.*
- Pavement damage using calibrated distress models & associated failure criterion (e.g., AC rutting & bottom-up FC, Unbound materials rutting)
- Calculate life reduction (LR) due to one pass of the heavy analysis truck.
- Calculate RSL based on time to & cost of planned next major structural repair.

$$PDAC\ (\$/lane-mile) = \left[\frac{Repair\ Cost\ per\ mile}{(1+Discount\ Rate)^{(n_f = yrs\ to\ reach\ failure\ criterion)}}\right] \times LR \times RSL$$

[1] Tirado, C., C. Carrasco, J.M. Mares, N. Gharaibeh, S. Nazarian, and J. Bendaña. Process to Estimate Permit Cost from Movement of Heavy Trucks on Flexible Pavements. In TRR: Journal of the Transportation Research Board, No 2154, Transportation Research Board of the national Academies, Washington, D.C., 2010, pp. 187-196.

Pavement Damage Associated Cost (PDAC)

- Multiple factors are considered when evaluating pavement damage from heavy vehicles
  - Vehicle speed
  - Axle load & configuration
  - Tire type & load
  - Pavement structure
  - Pavement temperature
  - Material properties
  - Existing pavement condition

Pavement Damage Associated Cost (Cont'd)

Overweight Vehicle
(80,000 lbs < GVW < 250,000 lbs)

↓

Pavement Damage Analysis using Pavement Response Database

↓

Cost Allocation Methodology

Superheavy Vehicle
(GVW ≥ 250,000 lbs)

↓

Case Specific Pavement Damage Analysis

↓

Cost Allocation Methodology

Pavement Response Database

- A broad range of conditions including:
  - Multiple pavement Structures
  - Geographical Location (**Material Properties**)
  - Pavement temperatures (**1-150°F**)
  - Vehicle speed (**1-90 mph**)
  - Multiple axle configurations/loads
  - Over 7,000 pavement analyses



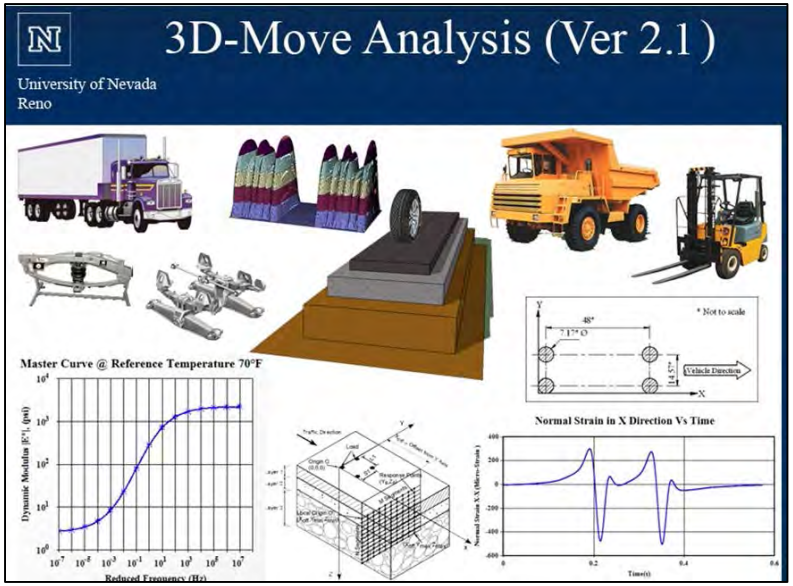
http://www.personalinjurylawyer.co/state-resources/Tuscaloosa-Personal-Injury-Lawyer-3130.html



http://www.bestchoicetireandservice.com/staying-on-the-road-all-summer-long/

Pavement Response Database (Cont'd)

- Using 3D-Move Analysis software developed at UNR.
  - frequency & temperature dependent material properties.
  - Moving vehicle at constant speed
  - Uniform/non-uniform tire contact pressure (Wide base tires).



PDAC Case Example 1: GVW = 110,250 lbs
Single Trip Analysis (Deterministic)

Permit

NEVADA DEPARTMENT OF TRANSPORTATION
1263 South Stewart Street, Carson City, Nevada 89712, 800-552-2127/775-888-7410

Permit # NDOT30477

OVER-DIMENSIONAL VEHICLE PERMIT

Permit Type:	TRIP - 5 DAY @ $25	GENERAL	BILLING
Insurance:	TRAVELERS GROUP		

AMERICAN TRANSPORT INC
100 INDUSTRY DRIVE
PITTSBURGH, PA, USA 15275

Route: From:	CALIFORNIA/NEVADA LINE
To:	NEVADA/ARIZONA LINE
Over Routes:	SR 164, US 95, SR 163
Instructions:	
Travel:	FROM 1/9/2014 THRU 1/13/2014
Authorized:	✓ Weekend ✓ Night ☐ Holiday ☐ Workday Commute Hour
Description of Load:	HAUL MILITARY VEHICLE
Dimensions:	**Width:** 10' 0" **Height:** Legal **Length:** 75' 0"
Gross Weight:	110,250 **Total Axles:** 5 **Overhang:** **Front:** Legal **Rear:** Legal

Axle Spacing	1	20' 7"	2	4' 6"	3	38' 9"	4	4' 6"	5
Wheels	4		4		4		4		4
Wgt	16,800 (Steer weight)		46,725				46,725		

Pilot Cars Required:	**Fore:** NONE REQUIRED
	Aft: NONE REQUIRED
Transmitted By:	EMAIL

Relevant Information

- *Axle Configuration/Loads*
  - Number of axles
  - Axle type, axle loads
- *Route*
  - Pavement structure
  - District (AC mixture)
  - Miles travelled = 57 miles
- *Date and Time of Move*
  - Pavement temperature estimations (**January**)
- *Vehicle Operational Speed*
  - 45 mph

PDAC Case Example 1: GVW = 110,250 lbs
Single Trip Analysis (Deterministic): Input

General Inputs

General Analysis Information

Selected Vehicle Operational Speed, mph

45

Number of Miles in OW Trip

120

Pavement Structure

6 AC - 10 CAB

Pavement Section AADTT

400

Environmental Conditions

OW Vehicle Pavement Damage and PDAC Calculation Sheet

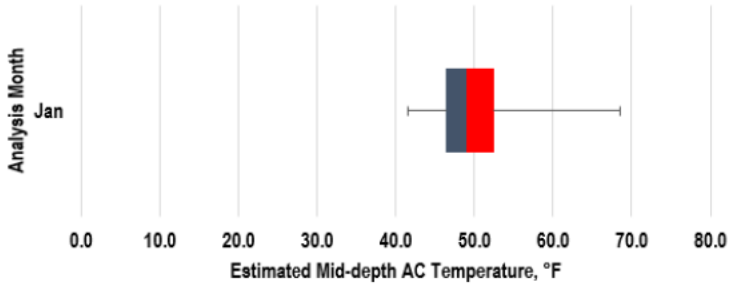
Climatic Information

Select the Climatic Station

Las Vegas

Month of OW Move

Jan



PDAC Case Example 1: GVW = 110,250 lbs
Single Trip Analysis (Deterministic): Input

Overweight Vehicle Axle Configuration

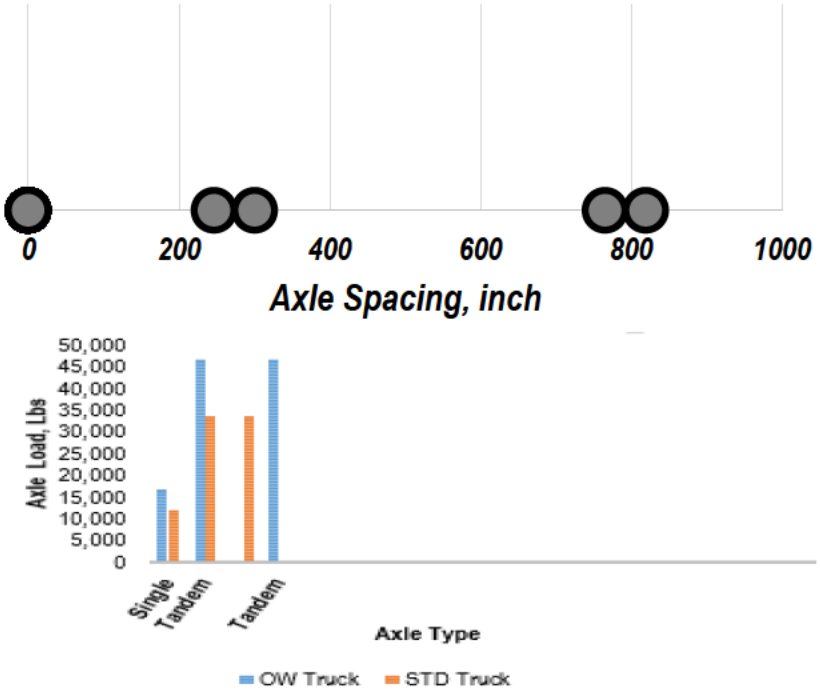
Total Gross Vehicle Weight, lbs

110,250

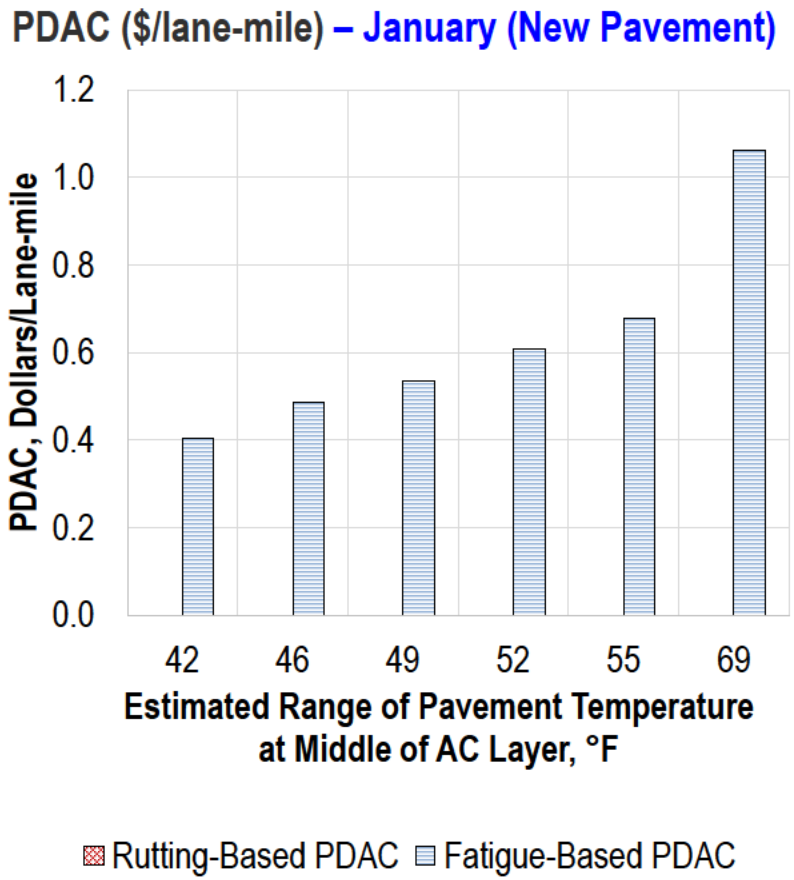
Number of Axles

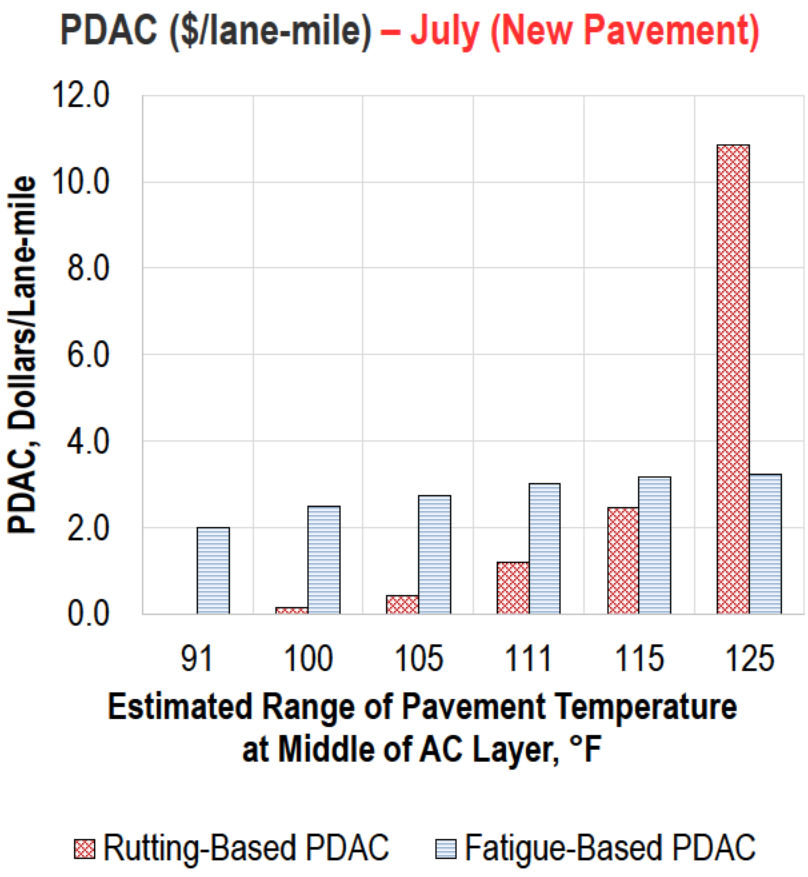
5

Axle	Number of Tires	Axle Spacing				Axle Load, lbs	Axle Type	Wide Base?
			ft	in	Total, in			
1	2	1-2	13	8	164	16,800	Single Axle Single Tires	-
2	4	2-3	4	6	54	46,725	Tandem Axle	-
3	4	3-4	13	8	164		-	-
4	4	4-5	5	4	64	46,725	Tandem Axle	-
5	4	-					-	-



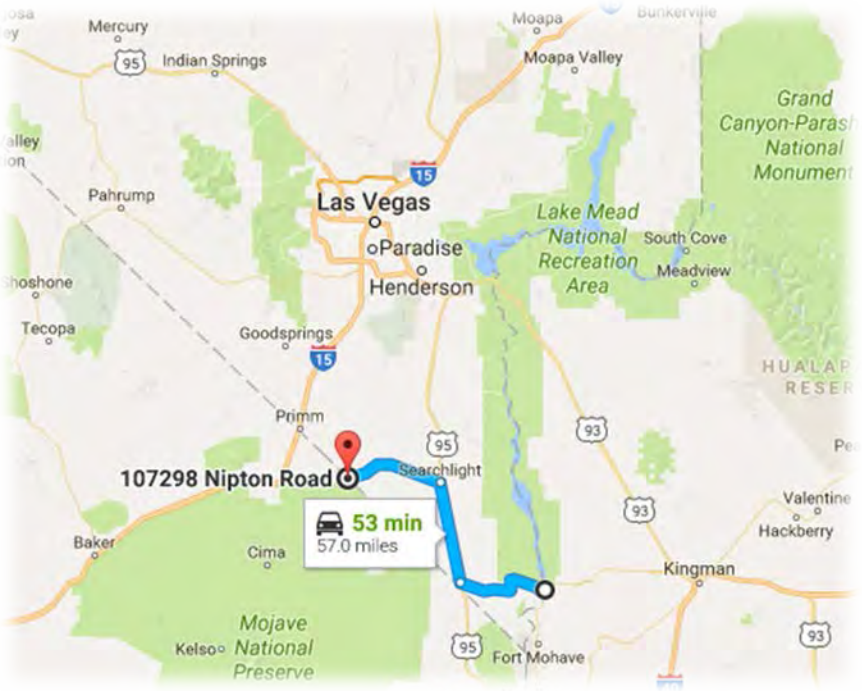
PDAC Case Example 1: GVW = 110,250 lbs
Single Trip Analysis (Deterministic): Output





PDAC Case Example 1: GVW = 110,250 lbs
Single Trip Analysis (Deterministic)

- Total Trip = 57 miles
- Trip Cost (RSL = 100%)
  - During Month of **January**: $23 to $61
  - During Month of July: $114 to $619



PDAC Case Example 2: GVW = 500,500 lbs
Single Trip Analysis (Deterministic)

Permit (assuming passed the SHL analyses for bearing capacity & service limit)

NEVADA DEPARTMENT OF TRANSPORTATION
1263 South Stewart Street, Carson City, Nevada 89712, 800-552-2127/775-888-7410

Permit # NDOT36584

OVER-DIMENSIONAL VEHICLE PERMIT

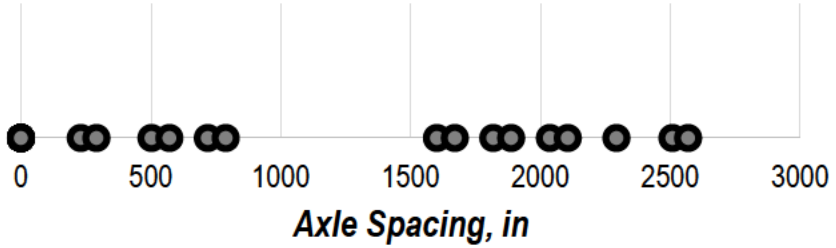
Permit Type:	TRIP - 5 DAY @ $25	GENERAL	CREDIT CARD
Insurance:			

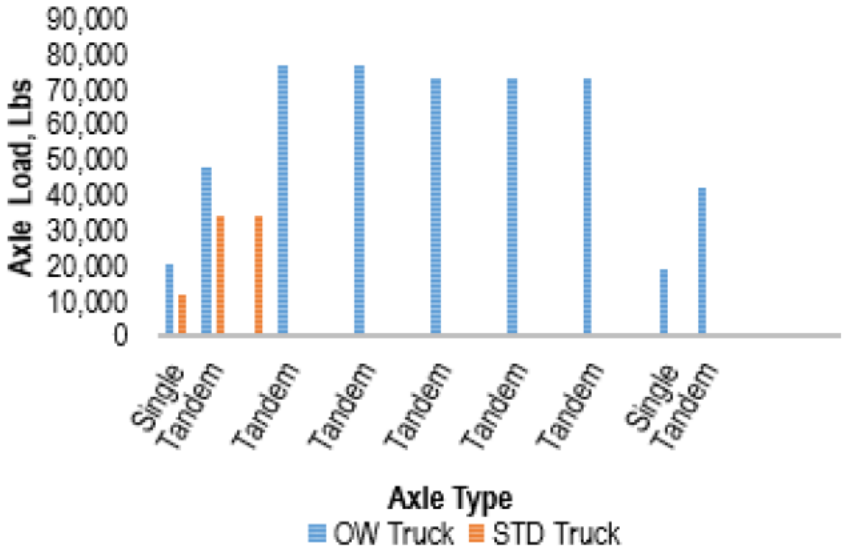
PERKINS SPECIALIZED TRANSPORTATION CONTRACTING
1800 RIVERVIEW DRIVE
NORTHFIELD, MN, USA 55051

Route:	**From:**	UTAH/NEVADA LINE
	To:	NEVADA/CALIFORNIA LINE
Over Routes:		US 6/50, US 6, US 6/95, US 6
Instructions:		***PERMITTEE TO USE CLEARANCE POLE TO CHECK HEIGHT. PERMITTEE RESPONSIBLE FOR CLEARING ALL STRUCTURES, UTILITY LINES AND SIGNALS; **NEVADA HIGHWAY PATROL ESCORT REQUIRED AND PLACEMENT OF UNITS LEFT TO THE DISCRETION OF NHP. **PERMITTEE HAS COMPLETED A ROUTE SURVEY--NEEDS COPY WITH PERMIT
Travel:		FROM 3/17/2014 THRU 3/21/2014
Authorized:		☐ Weekend ☐ Night ☐ Holiday ☐ Workday Commute Hour
Description of Load:		HAUL BOILER
Dimensions:	**Width:** 21' 2"	**Height:** 17' 3" **Length:** 222' 7"
Gross Weight:	500,500	**Total Axles:** 16 **Overhang:** **Front:** Legal **Rear:** Legal

Axle Spacing	1	19' 2"	2	5' 0"	3	17' 8"	4	5' 9"	5	12' 4"	6	5' 9"	7	57' 9"	8	5' 9"	9	12' 4"	10
Wheels	4		4		4		4		4		4		4		4		4		4
Wgt	20,000 (Steer weight)		47,500				76,500				76,500				73,000				

Axle Spacing	10	5' 9"	11	12' 5"	12	5' 9"	13	15' 8"	14	18' 0"	15	5' 0"	16						
Wheels	4		4		4		4		4		4		4						
Wgt		73,000 (Steer weight)				73,000				19,000		42,000							

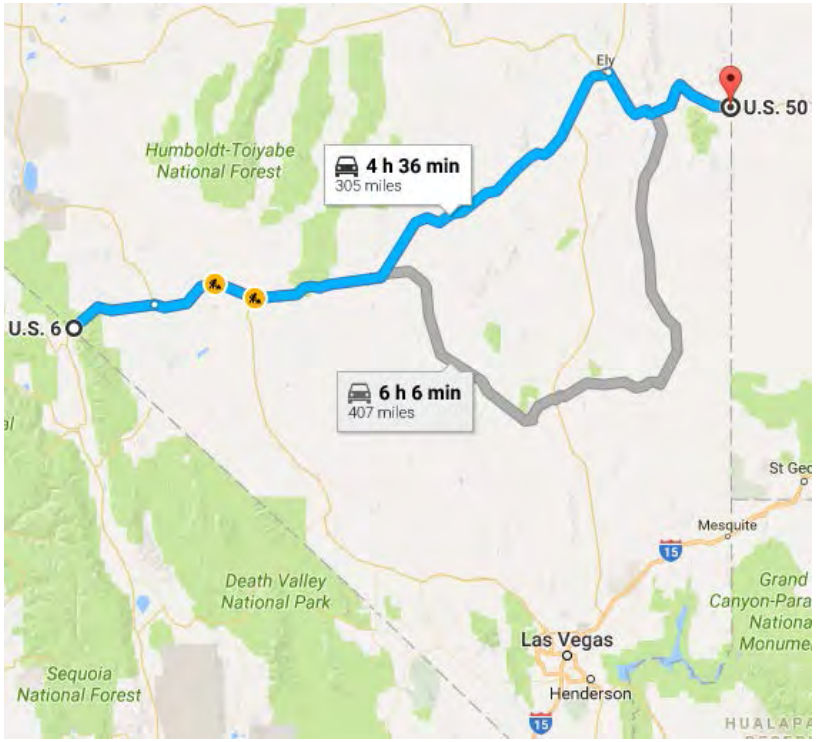




PDAC Case Example 2: GVW = 500,500 lbs
Single Trip Analysis (Deterministic)

- Total Trip = 305 miles

- Trip Cost (RSL = 100%)
  - During Month of **March**: (1.34-2.33)$/lane-mile×305 miles×2 lanes = $820 to $1,418
  - During Month of July: (2.59-12.28)$/lane-mile×305 miles×2 lanes = $1,577 to $7,491



(the 12.28 $/lane-mile corresponds to the maximum pavement temperature possible during the month of July. The 90th percentile corresponds to 4.38 $/lane-mile for a total of 2,670 $/trip)

PDAC
Multi-Trips Analysis (Probabilistic Approach)

- High degree of uncertainty is associated to OW multi-trips permits (i.e. Annual, semiannual permits)
  - Number of single trips associated to each multi-trip permit
  - Vehicle Miles Travelled (VMT)
  - Date and time of the year when the trips took place (*pavement temperature*)
  - Axle loads

- Considers variations in critical factors that might occur during the duration of the permit.
  - Thousands of Monte-Carlo simulations were conducted to generate OW case trucks traveling under various range of conditions encountered in Nevada.

PDAC (Cont'd)
Multi-Trips Analysis (Probabilistic Approach)

- **Monte-Carlo Simulations**
  - **Inputs:**
    - GVW, truck type, & Axle load distributions.
    - Hourly pavement temperature distribution in the middle of AC layer.
    - Pavement structure & material properties based on distribution of VMT on different road categories.
  - **Outputs:**
    - Critical pavement responses distribution.
    - PDAC distribution

- **PDAC can then be selected for any percentile level.**

Mutual Collaboration

- Solicit case studies
- List of input information/data for analysis can be shared with interested entities.

Questions?



Source: http://tspsalesandservice.com/scheuerle/inter-combi-trailer





Thank You!



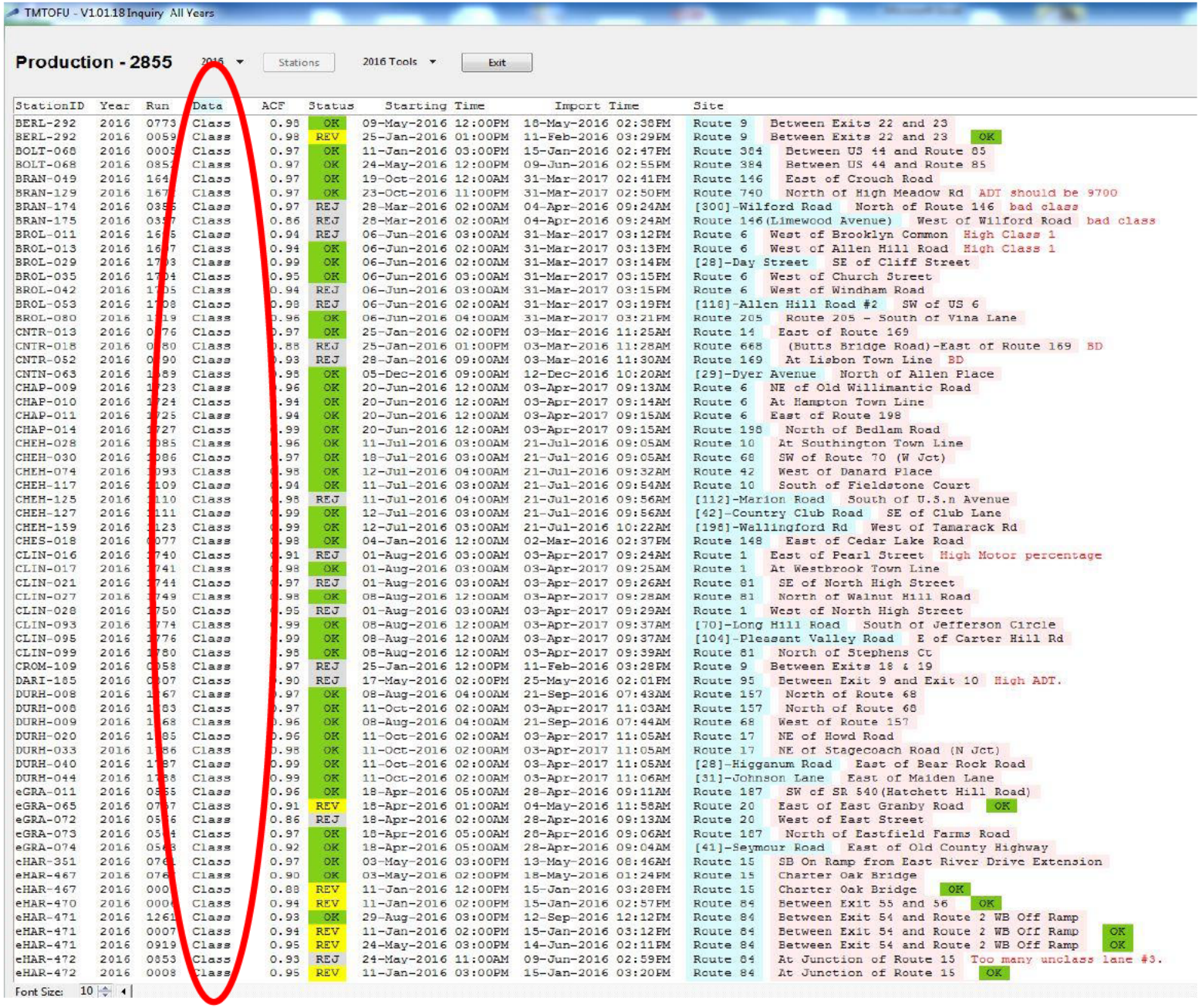
WIM Status – Traffic Monitoring

Brad Overturf –CTDOT Planning

5/24/2017

Related HPMS Requirement

H	I	J	K	L	M	N	O	P
		AADT-Sing	%Peak	AADT-	%Peak			Future
Length	AADT	Unit-Truck	Single-Truck	Comb-Truck	Comb-Truck	Kfactor	Dir Fac	AADT
0.030	27900	730	0.169	704	0.242			
0.060	21700	568	0.169	547	0.242			
0.120	17700	463	0.169	447	0.242			
0.520	20900	547	0.169	527	0.242			
0.700	20900	547	0.169	527	0.242	9	60	21100
0.160	19500	510	0.169	492	0.242			
0.160	20600	539	0.169	520	0.242			
0.590	17400	455	0.169	439	0.242			
0.320	20300	531	0.169	512	0.242			
0.480	21600	565	0.169	545	0.242			



TMTOFU - V1.01.18 Inquiry All Years

Production - 2855 2016 Stations 2016 Tools Exit

StationID	Year	Run	Data	ACF	Status	Starting Time	Import Time	Site
BERL-292	2016	0773	Class	0.98	OK	09-May-2016 12:00PM	18-May-2016 02:38PM	Route 9 Between Exits 22 and 23
BERL-292	2016	0059	Class	0.98	REV	25-Jan-2016 01:00PM	11-Feb-2016 03:29PM	Route 9 Between Exits 22 and 23 OK
BOLT-068	2016	0005	Class	0.97	OK	11-Jan-2016 03:00PM	15-Jan-2016 02:47PM	Route 384 Between US 44 and Route 85
BOLT-068	2016	0852	Class	0.97	OK	24-May-2016 12:00PM	09-Jun-2016 02:55PM	Route 384 Between US 44 and Route 85
BRAN-049	2016	164	Class	0.97	OK	19-Oct-2016 12:00AM	31-Mar-2017 02:41PM	Route 146 East of Crouch Road
BRAN-129	2016	167	Class	0.97	OK	23-Oct-2016 11:00PM	31-Mar-2017 02:50PM	Route 740 North of High Meadow Rd ADT should be 9700
BRAN-174	2016	0356	Class	0.97	REJ	28-Mar-2016 02:00AM	04-Apr-2016 09:24AM	[300]-Wilford Road North of Route 146 bad class
BRAN-175	2016	0357	Class	0.86	REJ	28-Mar-2016 02:00AM	04-Apr-2016 09:24AM	Route 146(Limewood Avenue) West of Wilford Road bad class
BROL-011	2016	1695	Class	0.94	REJ	06-Jun-2016 03:00AM	31-Mar-2017 03:12PM	Route 6 West of Brooklyn Common High Class 1
BROL-013	2016	1697	Class	0.94	OK	06-Jun-2016 02:00AM	31-Mar-2017 03:13PM	Route 6 West of Allen Hill Road High Class 1
BROL-029	2016	1703	Class	0.99	OK	06-Jun-2016 02:00AM	31-Mar-2017 03:14PM	[28]-Day Street SE of Cliff Street
BROL-035	2016	1704	Class	0.95	OK	06-Jun-2016 03:00AM	31-Mar-2017 03:15PM	Route 6 West of Church Street
BROL-042	2016	1705	Class	0.94	REJ	06-Jun-2016 03:00AM	31-Mar-2017 03:15PM	Route 6 West of Windham Road
BROL-053	2016	1708	Class	0.98	REJ	06-Jun-2016 02:00AM	31-Mar-2017 03:19PM	[118]-Allen Hill Road #2 SW of US 6
BROL-080	2016	1719	Class	0.96	OK	06-Jun-2016 04:00AM	31-Mar-2017 03:21PM	Route 205 Route 205 - South of Vina Lane
CNTR-013	2016	0776	Class	0.97	OK	25-Jan-2016 02:00PM	03-Mar-2016 11:25AM	Route 14 East of Route 169
CNTR-018	2016	0780	Class	0.88	REJ	25-Jan-2016 01:00PM	03-Mar-2016 11:28AM	Route 668 (Butts Bridge Road)-East of Route 169 BD
CNTR-052	2016	0790	Class	0.93	REJ	28-Jan-2016 09:00AM	03-Mar-2016 11:30AM	Route 169 At Lisbon Town Line BD
CNTN-063	2016	1689	Class	0.98	OK	05-Dec-2016 09:00AM	12-Dec-2016 10:20AM	[29]-Dyer Avenue North of Allen Place
CHAP-009	2016	1723	Class	0.96	OK	20-Jun-2016 12:00AM	03-Apr-2017 09:13AM	Route 6 NE of Old Willimantic Road
CHAP-010	2016	1724	Class	0.94	OK	20-Jun-2016 12:00AM	03-Apr-2017 09:14AM	Route 6 At Hampton Town Line
CHAP-011	2016	1725	Class	0.94	OK	20-Jun-2016 12:00AM	03-Apr-2017 09:15AM	Route 6 East of Route 198
CHAP-014	2016	1727	Class	0.99	OK	20-Jun-2016 12:00AM	03-Apr-2017 09:15AM	Route 198 North of Bedlam Road
CHEH-028	2016	1085	Class	0.96	OK	11-Jul-2016 03:00AM	21-Jul-2016 09:05AM	Route 10 At Southington Town Line
CHEH-030	2016	1086	Class	0.97	OK	18-Jul-2016 03:00AM	21-Jul-2016 09:05AM	Route 68 SW of Route 70 (W Jct)
CHEH-074	2016	1093	Class	0.98	OK	12-Jul-2016 04:00AM	21-Jul-2016 09:32AM	Route 42 West of Danard Place
CHEH-117	2016	1109	Class	0.94	OK	11-Jul-2016 03:00AM	21-Jul-2016 09:54AM	Route 10 South of Fieldstone Court
CHEH-125	2016	1110	Class	0.98	REJ	11-Jul-2016 04:00AM	21-Jul-2016 09:56AM	[112]-Marion Road South of U.S.n Avenue
CHEH-127	2016	1111	Class	0.99	OK	12-Jul-2016 03:00AM	21-Jul-2016 09:56AM	[42]-Country Club Road SE of Club Lane
CHEH-159	2016	1123	Class	0.99	OK	12-Jul-2016 03:00AM	21-Jul-2016 10:22AM	[198]-Wallingford Rd West of Tamarack Rd
CHES-018	2016	0077	Class	0.98	OK	04-Jan-2016 12:00AM	02-Mar-2016 02:37PM	Route 148 East of Cedar Lake Road
CLIN-016	2016	1740	Class	0.91	REJ	01-Aug-2016 03:00AM	03-Apr-2017 09:24AM	Route 1 East of Pearl Street High Motor percentage
CLIN-017	2016	1741	Class	0.98	OK	01-Aug-2016 03:00AM	03-Apr-2017 09:25AM	Route 1 At Westbrook Town Line
CLIN-021	2016	1744	Class	0.97	REJ	01-Aug-2016 03:00AM	03-Apr-2017 09:26AM	Route 81 SE of North High Street
CLIN-027	2016	1749	Class	0.98	OK	08-Aug-2016 12:00AM	03-Apr-2017 09:28AM	Route 81 North of Walnut Hill Road
CLIN-028	2016	1750	Class	0.95	REJ	01-Aug-2016 03:00AM	03-Apr-2017 09:29AM	Route 1 West of North High Street
CLIN-093	2016	1774	Class	0.99	OK	08-Aug-2016 12:00AM	03-Apr-2017 09:37AM	[70]-Long Hill Road South of Jefferson Circle
CLIN-095	2016	1776	Class	0.99	OK	08-Aug-2016 12:00AM	03-Apr-2017 09:37AM	[104]-Pleasant Valley Road E of Carter Hill Rd
CLIN-099	2016	1780	Class	0.95	OK	08-Aug-2016 12:00AM	03-Apr-2017 09:39AM	Route 81 North of Stephens Ct
CROM-109	2016	0058	Class	0.97	REJ	25-Jan-2016 12:00PM	11-Feb-2016 03:28PM	Route 9 Between Exits 18 & 19
DARI-185	2016	0007	Class	0.90	REJ	17-May-2016 02:00PM	25-May-2016 02:01PM	Route 95 Between Exit 9 and Exit 10 High ADT.
DURH-008	2016	1667	Class	0.97	OK	08-Aug-2016 04:00AM	21-Sep-2016 07:43AM	Route 157 North of Route 68
DURH-008	2016	1683	Class	0.97	OK	11-Oct-2016 02:00AM	03-Apr-2017 11:03AM	Route 157 North of Route 68
DURH-009	2016	1668	Class	0.96	OK	08-Aug-2016 04:00AM	21-Sep-2016 07:44AM	Route 68 West of Route 157
DURH-020	2016	1685	Class	0.96	OK	11-Oct-2016 02:00AM	03-Apr-2017 11:05AM	Route 17 NE of Howd Road
DURH-033	2016	1686	Class	0.98	OK	11-Oct-2016 02:00AM	03-Apr-2017 11:05AM	Route 17 NE of Stagecoach Road (N Jct)
DURH-040	2016	1687	Class	0.99	OK	11-Oct-2016 02:00AM	03-Apr-2017 11:05AM	[28]-Higganum Road East of Bear Rock Road
DURH-044	2016	1688	Class	0.99	OK	11-Oct-2016 02:00AM	03-Apr-2017 11:06AM	[31]-Johnson Lane East of Maiden Lane
eGRA-011	2016	0855	Class	0.96	OK	18-Apr-2016 05:00AM	28-Apr-2016 09:11AM	Route 187 SW of SR 540(Hatchett Hill Road)
eGRA-065	2016	0757	Class	0.91	REV	18-Apr-2016 01:00AM	04-May-2016 11:58AM	Route 20 East of East Granby Road OK
eGRA-072	2016	0516	Class	0.86	REJ	18-Apr-2016 02:00AM	28-Apr-2016 09:13AM	Route 20 West of East Street
eGRA-073	2016	0514	Class	0.97	OK	18-Apr-2016 05:00AM	28-Apr-2016 09:06AM	Route 187 North of Eastfield Farms Road
eGRA-074	2016	0568	Class	0.92	OK	18-Apr-2016 05:00AM	28-Apr-2016 09:04AM	[41]-Seymour Road East of Old County Highway
eHAR-351	2016	0761	Class	0.97	OK	03-May-2016 03:00PM	13-May-2016 08:46AM	Route 15 SB On Ramp from East River Drive Extension
eHAR-467	2016	0760	Class	0.90	OK	03-May-2016 02:00PM	18-May-2016 01:24PM	Route 15 Charter Oak Bridge
eHAR-467	2016	0001	Class	0.88	REV	11-Jan-2016 12:00PM	15-Jan-2016 03:28PM	Route 15 Charter Oak Bridge OK
eHAR-470	2016	0004	Class	0.94	REV	11-Jan-2016 02:00PM	15-Jan-2016 02:57PM	Route 84 Between Exit 55 and 56 OK
eHAR-471	2016	1261	Class	0.93	OK	29-Aug-2016 03:00PM	12-Sep-2016 12:12PM	Route 84 Between Exit 54 and Route 2 WB Off Ramp
eHAR-471	2016	0007	Class	0.94	REV	11-Jan-2016 02:00PM	15-Jan-2016 03:12PM	Route 84 Between Exit 54 and Route 2 WB Off Ramp OK
eHAR-471	2016	0919	Class	0.95	REV	24-May-2016 03:00PM	14-Jun-2016 02:11PM	Route 84 Between Exit 54 and Route 2 WB Off Ramp OK
eHAR-472	2016	0853	Class	0.93	REJ	24-May-2016 11:00AM	09-Jun-2016 02:59PM	Route 84 At Junction of Route 15 Too many unclass lane #3.
eHAR-472	2016	0008	Class	0.95	REV	11-Jan-2016 03:00PM	15-Jan-2016 03:20PM	Route 84 At Junction of Route 15 OK

Font Size: 10

Status
REV

North | Lane 1 | Lane 2 | Lane 3 | Lane 4 | Volume

nwLO-287 - North

Route 95 - 93.52 mi The Gold Star Bridge

Town.....New London
Station.....287
Location..... 41.364098,-72.088159
A.K.A.....1959
2015-Interstate 1.....2015-Urban
Start Report.....19-Jan-2016 12:00AM
All Vehicle Peak Hour.....20-Jan-2016 04:00PM
End Report.....21-Jan-2016 11:00PM
Annualized ADT.....55900
REV 2017 Tue 11-Apr 7900
REJ 2016 Mon 04-Jan 52900
REV 2016 Tue 19-Jan -this report-.....55900
REV 2015 Tue 06-Oct 41200
RAW 2008 Tue 03-Jun 49400
Dataset Details.....1

	Count	Percent	Axles
Motorcycles	44	0.03%	88
Passenger Cars	126729	85.01%	253458
Four-Tire Vehicles	13740	9.22%	27480
Light Vehicle Totals	140513	94.25%	281026
Buses	95	0.06%	190
Single-Unit Trucks			
Six-Tire Trucks	2092	1.40%	4184
Three-Axle Trucks	561	0.38%	1683
Four-Axle Trucks	106	0.07%	424
Single-Trailer Trucks			
Four or Less Axles	571	0.38%	2284
Five Axles	4891	3.28%	24455
Six or More Axles	37	0.02%	222
Multi-Trailer Trucks			
Five Axles or Less	152	0.10%	760
Six Axles	36	0.02%	216
Seven or More Axles	27	0.02%	189
Heavy Vehicle Totals	8568	5.75%	34607
Total Classified	149081	95.02%	315633
Total Unclassified	7807	4.98%	
Total Vehicles	156888		

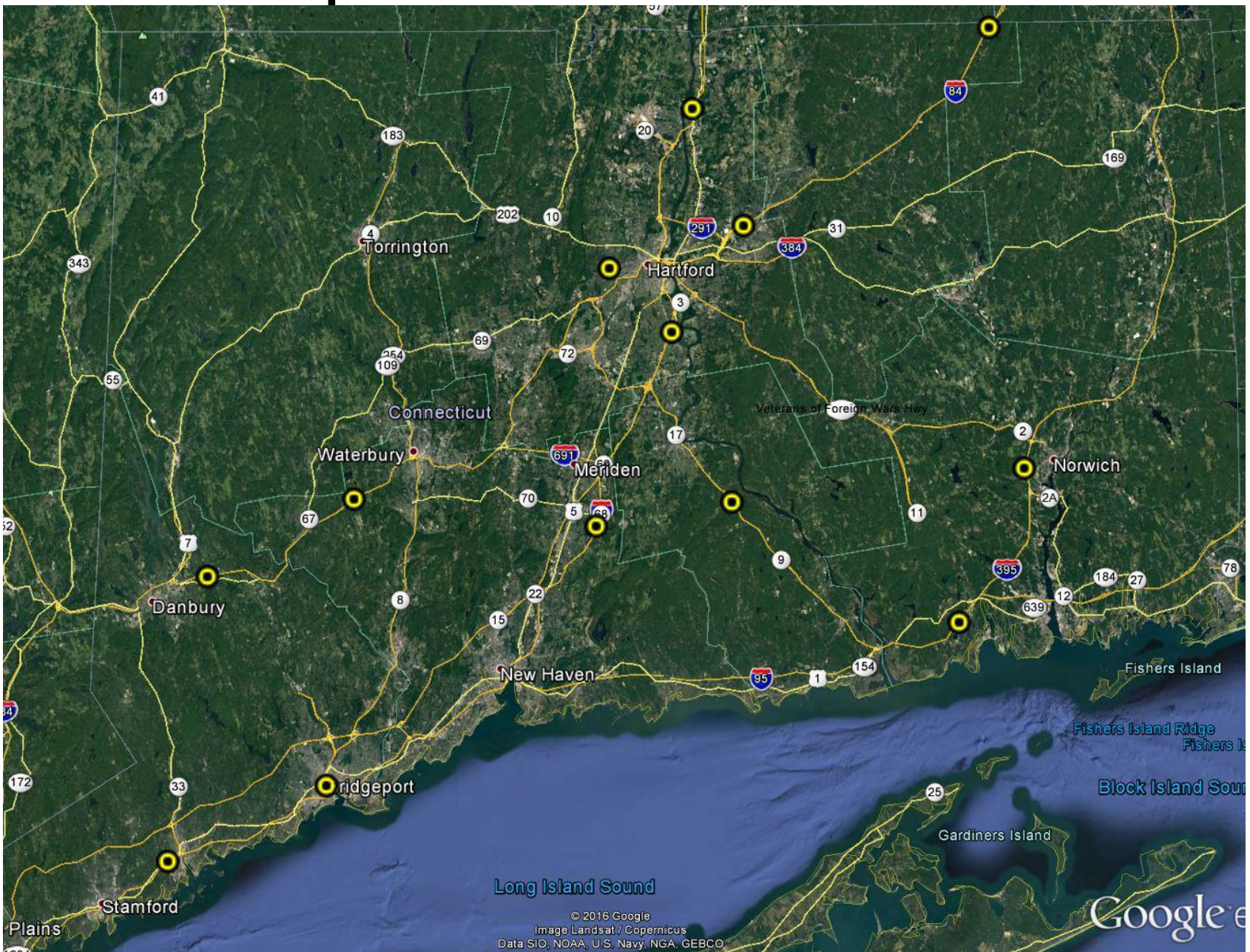
Road-Tube Equivalent.....157816
Axle Correction Factor.....0.94
All Vehicle Peak Hour Volume.....4058

	Single	Combo
Peak Hour Truck Volume	43	401
% Total Peak Hour Volume	1.1%	9.9%
24 Hour Truck Volume	930	4525
All-Vehicle Annualized ADT	55900	55900
24Hour T-Vol % of A-V AADT	1.7%	8.1%
PeakHr T-Vol % of A-V AADT	0.1%	0.7%
K-Factor (Peak/AADT)	7.3%	7.3%

(AADT & Legacy AADT match)

Hour	Motor Cycle	Pass Cars	4 Tire	Buses	6 Tire	3 Axles	4 Axles	4 or Less Axles	5 Axles	6 or More Axles	5 or Less Axles	6 Axles	7 or More Axles	Un-Class	Time Span Total
19-Jan Tue															
12:00am	.	308	23	.	6	1	1	4	47	.	4	.	.	.	394
01:00am	.	149	10	.	6	1	1	5	69	.	.	.	.	.	241
02:00am	1	178	7	.	4	3	.	3	52	.	6	1	.	.	255
03:00am	.	205	17	.	6	1	.	8	56	.	5	.	.	.	298
04:00am	2	439	72	1	18	7	.	11	75	.	3	2	1	.	631
05:00am	2	1437	234	.	25	3	.	10	81	.	8	2	.	.	1802
06:00am	1	2417	426	2	37	10	.	16	105	1	7	1	.	160	3183
07:00am	.	2964	348	3	50	13	.	14	82	1	1	.	1	387	3864
08:00am	2	2840	311	2	65	18	14	6	85	.	1	.	1	284	3629
09:00am	.	2199	229	3	67	22	.	10	46	.	.	.	1	135	2712
10:00am	2	2032	257	3	48	18	4	10	52	.	.	1	1	28	2456
11:00am	.	2296	283	1	46	25	1	14	79	.	1	.	2	93	2841
12:00pm	2	2378	285	2	43	17	7	11	89	1	.	.	.	144	2979
01:00pm	1	2420	281	4	61	20	3	7	91	.	2	1	1	193	3085
02:00pm	.	2656	319	2	47	19	1	12	73	2	1	.	2	271	3405
03:00pm	2	2863	317	1	35	14	1	6	62	1	.	.	.	240	3542
04:00pm	.	3236	307	1	36	3	1	4	45	.	.	.	.	367	4000
05:00pm	.	3126	245	2	23	4	2	3	36	1	.	.	1	213	3656
06:00pm	.	2401	171	2	16	3	1	3	54	.	1	1	.	89	2742
07:00pm	1	1561	139	.	11	.	1	.	44	.	.	.	.	.	1757
08:00pm	.	1386	84	2	9	2	.	3	69	1	.	2	.	.	1558
09:00pm	.	1124	76	3	11	.	.	7	54	.	2	.	.	.	1277
10:00pm	.	723	50	.	3	.	.	3	56	.	2	1	.	.	838
11:00pm	.	474	34	.	5	.	.	6	46	1	2	.	.	.	568
Totals	16	41812	4525	34	678	204	38	176	1548	9	46	12	11	2604	51713
Percent	0.03	80.85	8.75	0.07	1.31	0.39	0.07	0.34	2.99	0.02	0.09	0.02	0.02	5.04	
20-Jan Wed															
12:00am	.	375	27	2	.	2	.	6	61	.	5	.	.	.	478
01:00am	.	191	5	1	8	.	.	4	65	.	4	1	.	.	279
02:00am	.	163	12	.	6	3	.	5	59	1	5	.	.	.	254
03:00am	.	211	13	.	11	1	.	4	62	.	4	.	.	.	306
04:00am	3	479	64	1	19	5	.	11	69	2	5	3	.	.	661
05:00am	.	1441	241	.	24	4	.	17	104	2	10	1	.	.	1844
06:00am	1	2319	371	1	59	13	1	20	110	.	3	1	.	302	3201
07:00am	1	2882	361	1	55	12	2	8	89	1	3	.	1	252	3668
08:00am	.	2813	342	2	73	14	8	9	71	.	.	.	1	268	3601
09:00am	.	2201	267	1	69	10	9	7	67	1	.	1	.	168	2801
10:00am	1	1981	277	1	56	9	1	10	64	1	1	.	1	35	2438
11:00am	.	2185	231	4	42	15	2	10	79	1	.	.	2	186	2757
12:00pm	1	2254	251	1	46	12	11	13	97	1	2	.	.	173	2862
01:00pm	1	2326	285	3	47	14	7	8	95	3	.	2	.	92	2883
02:00pm	1	2650	318	2	49	11	1	7	74	.	1	.	.	178	3292
03:00pm	1	2869	309	.	31	2	1	14	71	.	.	.	1	306	3605
04:00pm	.	3270	344	1	38	1	3	4	55	.	.	.	1	341	4058
05:00pm	.	3204	308	1	30	1	.	4	55	.	1	.	1	218	3823
06:00pm	.	2427	194	2	13	1	1	5	44	.	1	1	.	54	2743
07:00pm	.	1768	125	1	15	3	1	.	45	1	.	.	.	.	1959
08:00pm	.	1377	96	.	11	1	1	1	66	.	.	1	.	.	1554
09:00pm	.	1181	71	.	8	.	.	12	64	.	2	.	.	.	1338
10:00pm	1	753	40	.	6	1	.	4	67	.	1	.	.	.	873
11:00pm	.	482	30	.	5	.	.	12	40	1	1	1	.	.	572
Totals	11	41802	4582	25	721	135	49	195	1673	15	49	12	8	2573	51850
Percent	0.02	80.62	8.84	0.05	1.39	0.26	0.09	0.38	3.23	0.03	0.09	0.02	0.02	4.96	
21-Jan															

WIM Capable Continuous Stations



Ad-Hoc Rpts | Graphs/Rpts

List View | All DIRs | Report Center | Save Search | Load Search | Build Search

Record 1 of 1 Goto Record go

Location ID	008052 Edit ID	MPO ID	DARI-018
Type	SPOT	HPMS ID	035J106
On NHS		On HPMS	Yes
LRS ID		LRS Loc Pt.	
SF Group		Route Type	
AF Group		Route	95
GF Group			
Class Dist Grp			
WIM Group			
QC Group	WIM		
Fnct'l Class	Interstate	Milepost	
Located On	95		
Loc On Alias			
	Between exits 9 - 10		

PR	MP	PT

More Detail

Edit WIM Settings

STATION DATA

Directions: 2-WAY | NB 1 2 3 | SB 1 2 3 4

AADT

	Year	AADT	DHV-30	K %	D %	PA	BC	Src
⊞								

Travel Demand Model

Model Year	Model AADT	AM PHV	AM PPV	MD PHV	MD PPV	PM PHV	PM PPV	NT PHV	NT PPV

VOLUME COUNT

View All

	Date	Int	Total	Status
	No Data			

Create | Flag/Unflag | Edit Multiple | Export Totals

VOLUME TREND

Year	Annual Growth

SPEED

View All

	Date	Int	Pace	85th	Total	Status
	No Data					

Create

CLASSIFICATION

View All

	Date	Int	Total	Status
	No Data			

Create

WEIGH-IN-MOTION

Graphs/Rpts

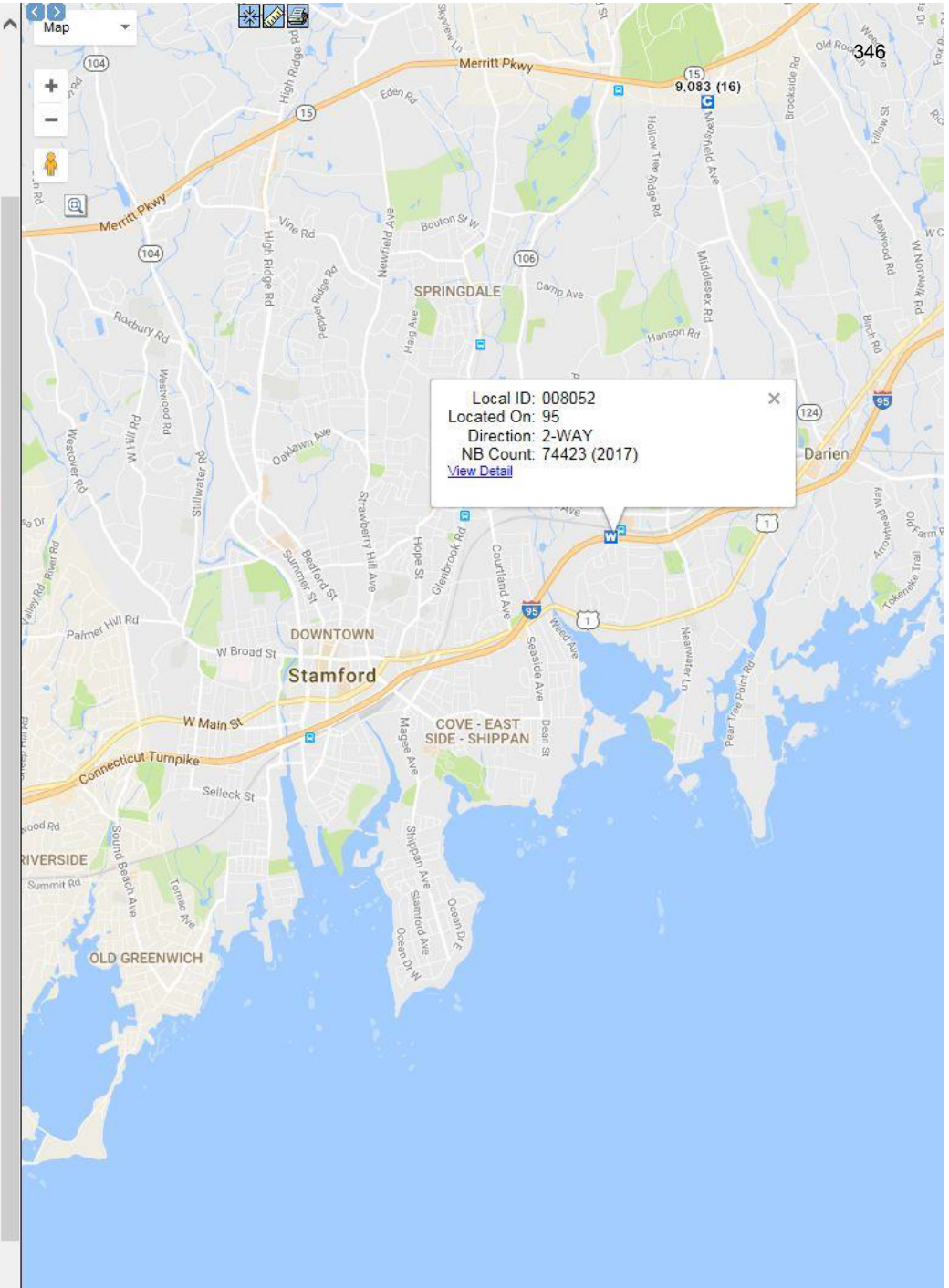
	Date	Axles	Avg GVW	Total	Status
👁	Fri 3/10/2017	61,748	12.31	25,021	✔
👁	Thu 3/9/2017	170,562	9.59	74,423	✔
👁	Wed 3/8/2017	183,374	9.09	80,694	✔
👁	Tue 3/7/2017	179,498	8.43	79,241	✔
👁	Mon 3/6/2017	176,723	8.33	78,660	✔
👁	Sun 3/5/2017	151,774	5.65	71,903	✔
👁	Sat 3/4/2017	169,428	5.83	80,404	✔
👁	Fri 3/3/2017	187,879	7.87	84,560	✔
👁	Thu 3/2/2017	184,975	8.52	81,389	✔
👁	Wed 3/1/2017	181,213	8.79	79,748	✔

|<< < > >>| 1-10 of 35

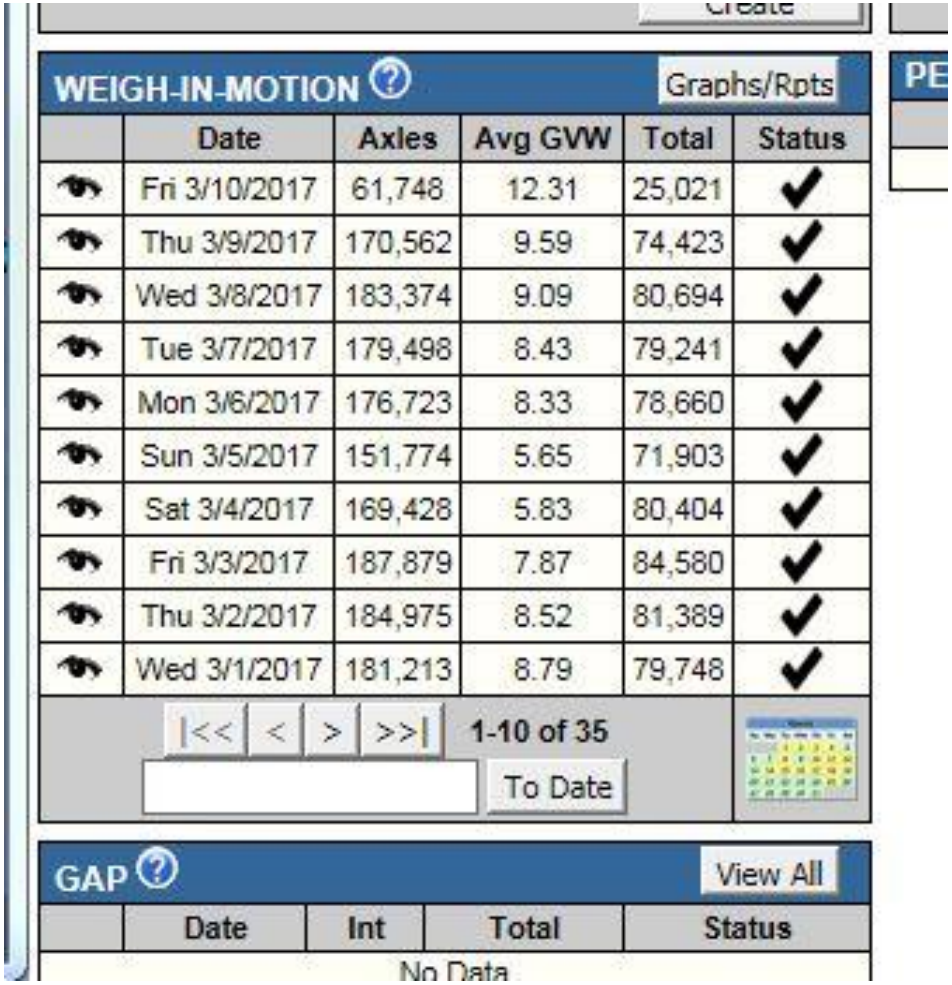
To Date

PER VEHICLE

	Date	Axles	85th	Total	Status
	No Data				



Available Data



WEIGH-IN-MOTION

Graphs/Rpts

	Date	Axles	Avg GVW	Total	Status
	Fri 3/10/2017	61,748	12.31	25,021	✔
	Thu 3/9/2017	170,562	9.59	74,423	✔
	Wed 3/8/2017	183,374	9.09	80,694	✔
	Tue 3/7/2017	179,498	8.43	79,241	✔
	Mon 3/6/2017	176,723	8.33	78,660	✔
	Sun 3/5/2017	151,774	5.65	71,903	✔
	Sat 3/4/2017	169,428	5.83	80,404	✔
	Fri 3/3/2017	187,879	7.87	84,580	✔
	Thu 3/2/2017	184,975	8.52	81,389	✔
	Wed 3/1/2017	181,213	8.79	79,748	✔

|<< < > >>| 1-10 of 35

To Date

GAP

View All

Date	Int	Total	Status
No Data			

Per-Vehicle Data

Per-Vehicle Raw Data

Row Formatting:
Invalid Vehicle
Warning Flag
Overweight vehicle

Time	Err	Dir	Ln	Class	Speed	GVW	Axles	Wgt A	Spc AB	Wgt B	Spc BC	Wgt C	Spc CD	Wgt D	Spc DE	Wgt E	Spc EF	Wg F
12:00:02 AM		NB	2	02	50	6.4	0											
12:00:02 AM		NB	1	09	70	31.1	5	3.3	17.8	7.6	4.5	7.6	34.7	6.3	4.2	6.4		
12:00:02 AM		NB	2	01	50	0.3	2	0.2	3.1	0.1								
12:00:03 AM		NB	2	12	71	42.6	6	8.4	17.0	6.2	4.4	6.9	20.8	7.8	9.0	6.7	23.1	6.5
12:00:04 AM		NB	1	02	59	2.0	2	1.0	10.1	1.0								
12:00:09 AM		NB	2	08	65	25.3	4	7.0	13.9	8.1	29.8	5.1	4.1	5.0				
12:00:11 AM		NB	1	02	66	2.6	2	1.3	9.3	1.2								
12:00:15 AM		NB	3	02	72	3.8	2	2.1	8.8	1.7								
12:00:18 AM		NB	3	02	75	2.6	2	1.4	8.5	1.2								
12:00:21 AM		NB	2	09	63	42.3	5	7.7	16.8	11.4	4.6	10.6	33.9	6.2	4.3	6.5		
12:00:22 AM		NB	1	02	56	2.6	2	1.3	8.5	1.3								
12:00:25 AM		NB	1	02	53	2.1	2	1.2	9.3	0.9								
12:00:27 AM		NB	2	02	73	1.1	2	0.6	9.2	0.5								
12:00:27 AM		NB	2	02	73	2.3	2	1.6	8.9	0.7								
12:00:27 AM		NB	3	02	69	4.2	2	2.3	9.9	1.9								
12:00:31 AM		NB	1	11	64	36.3	5	5.2	13.3	7.2	21.9	9.5	9.2	6.0	22.5	8.4		
12:00:32 AM		NB	3	05	68	9.6	2	5.8	14.3	3.8								
12:00:35 AM		NB	1	08	61	25.5	4	5.2	12.7	5.7	4.3	5.1	18.5	9.4				
12:00:36 AM	✗	**NB**	**2**	**09**	**58**	**65.3**	**5**	**7.5**	**17.2**	**13.5**	**4.3**	**14.2**	**28.3**	**14.0**	**4.0**	**16.0**		
12:00:38 AM		NB	2	02	67	1.5	2	0.9	9.1	0.6								
12:00:39 AM		NB	3	02	71	3.4	2	2.0	8.7	1.4								
12:00:42 AM		NB	3	02	68	2.9	2	1.7	8.6	1.3								
12:00:51 AM		NB	2	03	64	3.3	2	1.7	11.8	1.6								
12:00:53 AM		NB	2	02	64	1.1	2	0.7	10.1	0.4								
12:00:55 AM		NB	2	11	65	51.6	5	7.6	13.2	12.2	21.4	11.7	9.6	11.2	22.2	8.9		

Basic Graphs/Reports Option



Average Weight by Class

e Weight by Class													
Class													
C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15
26775	926	16	49	5	0	3	2	0	0	0	0	0	0
33557	5335	20	421	7	0	29	19	0	0	0	0	0	0
277	1871	41	610	16	0	26	27	1	0	1	0	0	0
8	188	150	307	28	0	25	32	0	3	0	0	0	0
4	27	369	170	57	1	31	57	0	1	0	1	0	0
0	21	220	119	51	0	41	103	4	3	3	0	0	0
3	7	110	60	76	1	76	173	1	4	2	0	0	0
5	5	68	22	69	0	81	324	2	6	2	0	0	0
1	3	54	9	41	1	96	519	2	12	0	0	0	0
0	1	51	1	31	4	76	523	2	8	1	0	0	0
1	1	67	1	11	1	64	517	0	8	7	0	0	0
2	0	19	0	13	9	42	439	3	17	8	0	0	0
1	0	4	0	4	6	29	405	3	18	8	0	0	0
0	0	4	0	0	6	13	377	2	22	10	0	0	0
0	0	1	0	0	16	7	340	2	32	11	0	0	0
0	0	2	0	0	10	2	367	2	25	13	0	0	0
0	0	0	0	0	16	1	427	2	17	11	0	0	0
0	0	0	0	0	10	1	580	3	14	12	0	0	0
0	0	0	0	0	7	1	497	6	9	2	0	0	0
0	0	0	0	0	1	0	265	4	1	0	0	0	0
1	0	0	0	0	4	0	172	5	4	1	0	0	0
60635	**8385**	**1196**	**1769**	**409**	**93**	**644**	**6165**	**44**	**204**	**92**	**1**	**0**	**0**

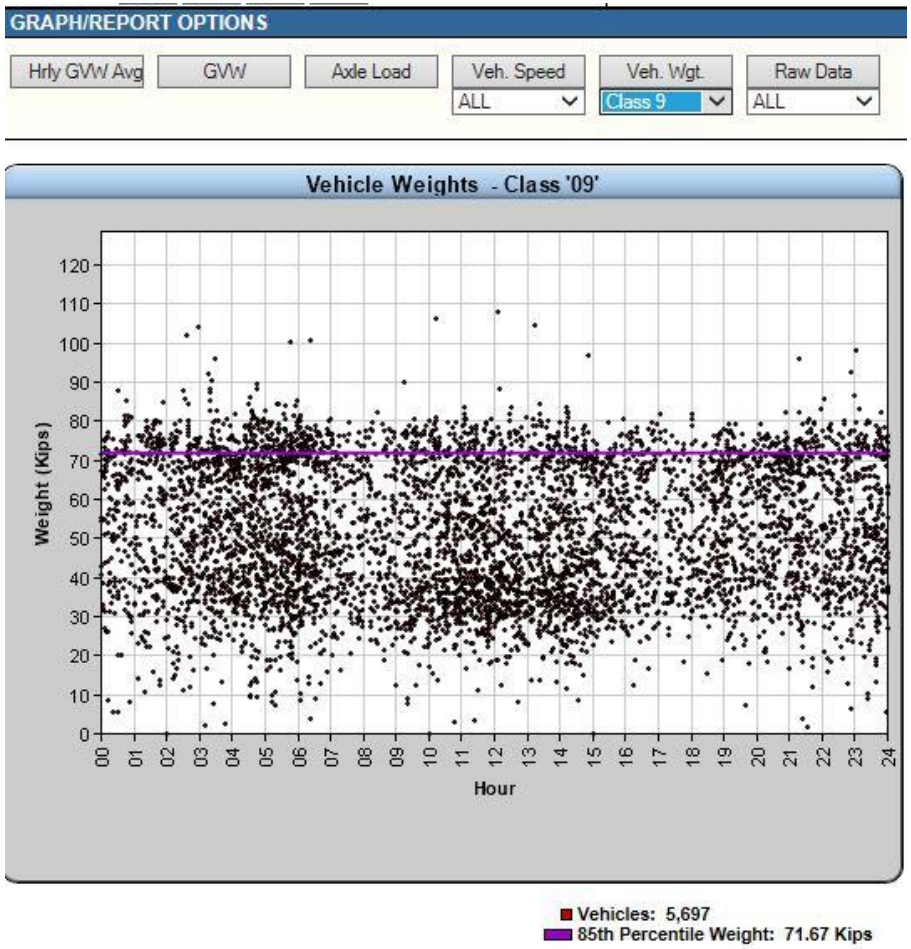
Axle Load by Class

Single | Tandem | Tridem | Quad | ESALs

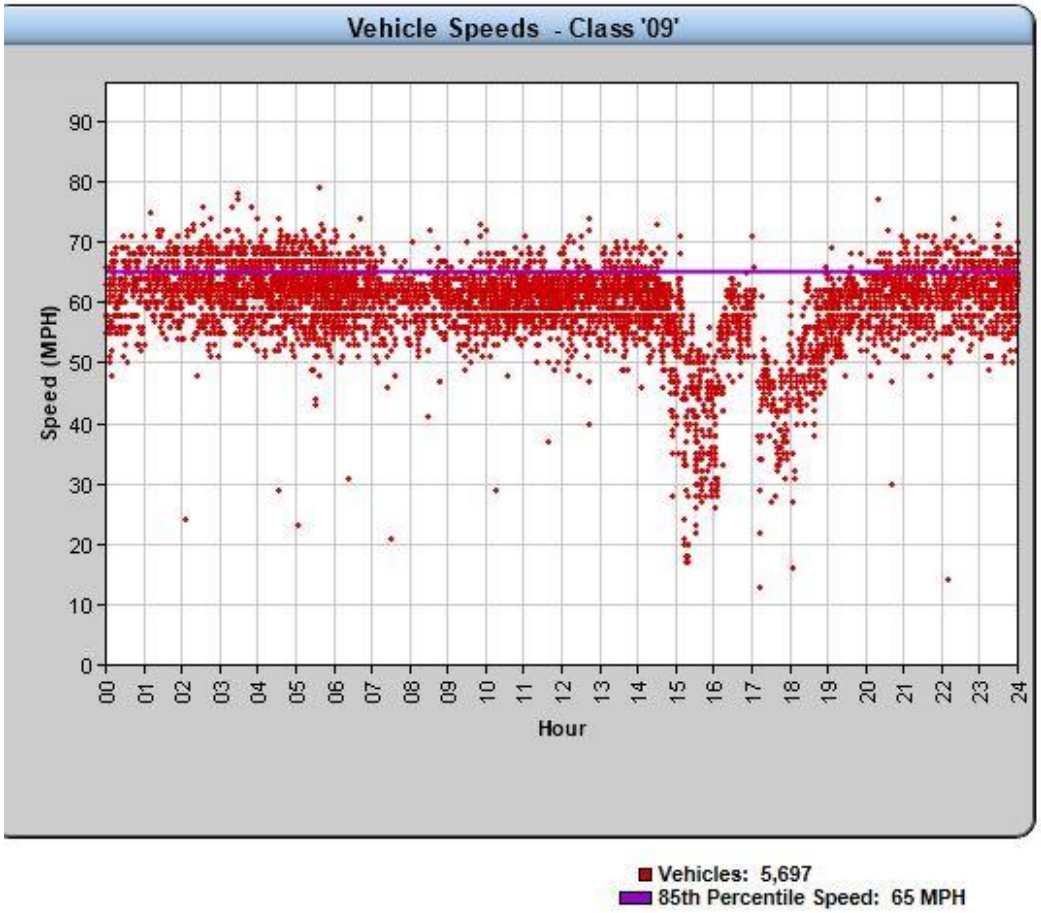
Axle Load by Class - TANDEM AXLES

Axle Load (kips)	Rigid	Flex	Class									
			C4	C5	C6	C7	C8	C9	C10	C11	C12	C13
0-4	0.000502	0.000223	10	37	10	0	18	70	1	0	1	1
4-8	0.005319	0.002577	4	32	40	0	57	343	4	0	4	1
8-12	0.025173	0.012868	11	5	72	0	119	1355	4	0	7	0
12-16	0.080378	0.042617	21	2	109	0	151	2098	6	0	25	0
16-20	0.203070	0.110285	27	0	82	0	110	1715	5	0	38	0
20-24	0.439078	0.241809	40	0	44	0	53	1503	4	0	16	0
24-28	0.849473	0.470057	61	0	24	0	20	1536	12	0	1	0
28-32	1.511259	0.833750	0	0	0	0	0	0	0	0	0	0
32-36	2.518257	1.374570	12	0	8	0	1	1023	1	0	0	0
36-40	3.977725	2.136296	2	0	2	0	0	197	3	0	0	0
40-44	6.009615	3.161555	1	0	0	0	0	38	1	0	0	0
44-48	8.748906	4.490346	2	0	0	0	0	15	0	0	0	0
48-52	12.315271	6.165228	0	0	0	0	0	1	0	0	0	0
52-56	16.835017	8.223684	0	0	0	0	0	0	0	0	0	0
56-60	22.471910	10.718114	0	0	0	0	0	0	0	0	0	0
60-64	29.325513	13.679891	0	0	0	0	0	0	0	0	0	0
64-68	37.453184	17.182131	0	0	0	0	0	0	0	0	0	0
68-72	47.169811	21.321962	0	0	0	0	0	0	0	0	0	0
72-76	58.479532	26.109661	0	0	0	0	0	0	0	0	0	0
76-80	71.942446	31.645570	0	0	0	0	0	0	0	0	0	0
80-84	87.719298	38.167939	0	0	0	0	0	0	0	0	0	0
84-88	105.263158	45.454545	0	0	0	0	0	0	0	0	0	0
89	109.890110	47.619048	0	0	0	0	0	0	0	0	0	0
Total			**191**	**76**	**391**	**0**	**529**	**9894**	**41**	**0**	**92**	**2**
ESALs - Rigid			**138.536**	**0.475**	**95.251**	**0**	**80.561**	**6249.294**	**34.031**	**0**	**17.798**	**0.005**
ESALs - Flexible			**75.282**	**0.24**	**51.91**	**0**	**43.84**	**3403.026**	**18.422**	**0**	**9.695**	**0.002**

Scatter Plots



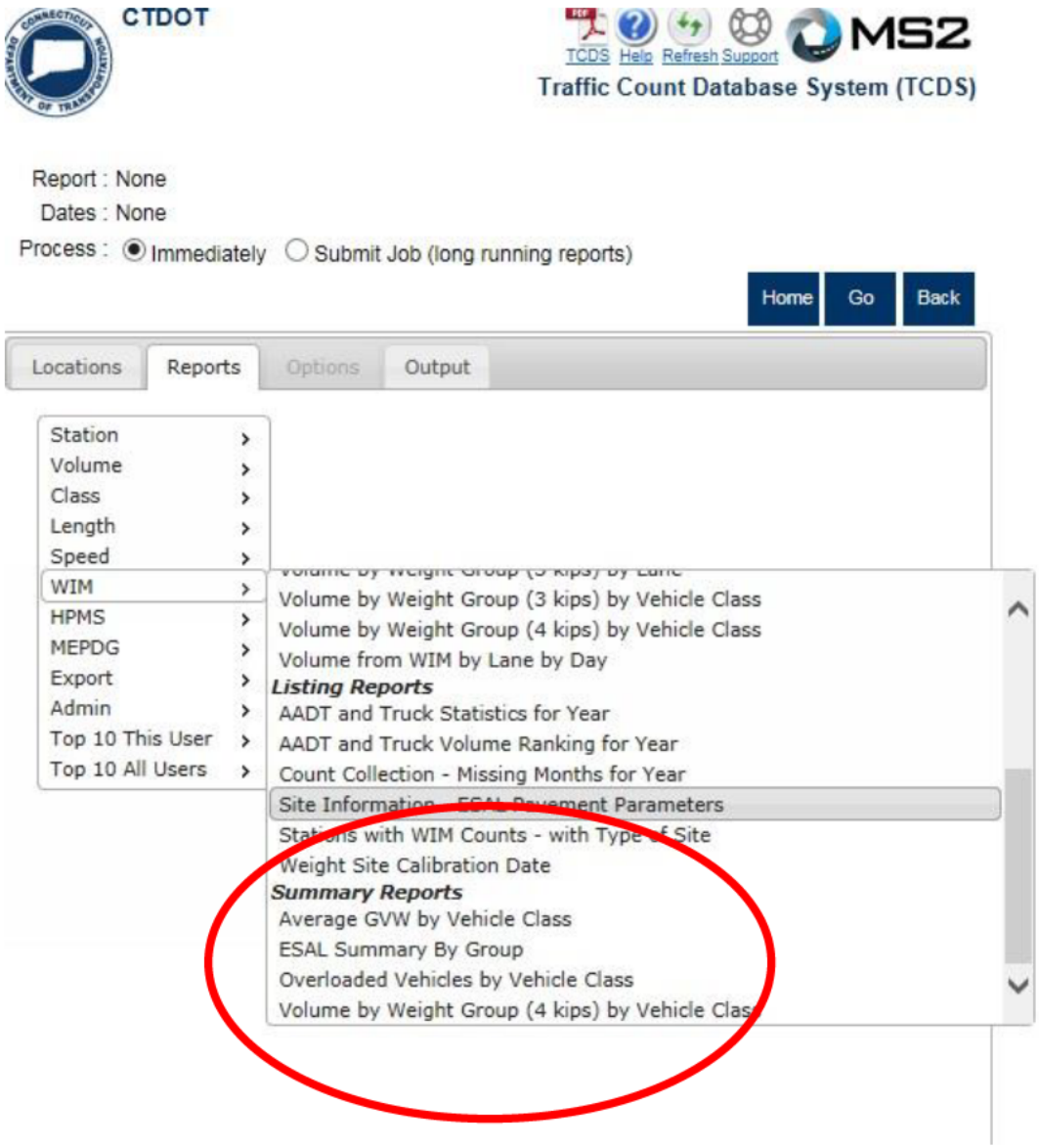
Speed Example by Class



Available Reports



Summary Reports

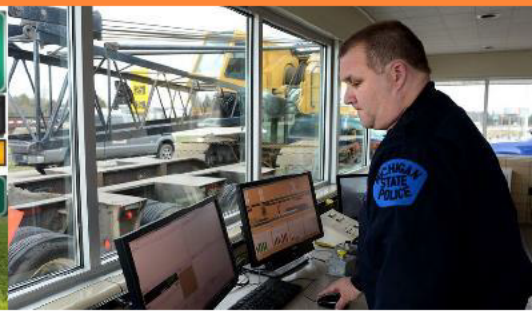


Automated Enforcement in the ITS environment









Smart Roadside Initiative (SRI) Impacts Assessment

Presented by

Sam Fayez

DEPARTMENT OF TRANSPORTATION UNITED STATES OF AMERICA

PRODUCTIVITY APEX INC.

Agenda

- Project Background
- Technologies Evaluated
- Sites Evaluated
- Objectives of Assessment
- Data Analysis Methodology
- Data Analysis of Sites
- Stakeholder Surveys
- Simulation
- Conclusion

© 2016 Productivity Apex, Inc.

Project Background

- This is an independent assessment of the effectiveness and lessons learned from roadside motor carrier compliance technologies including testing of the smart roadside technologies
- The objective is to analyze the impact of automated tools on truck enforcement personnel productivity, effectiveness, and efficiency.
- This Project is supported by:
  - Federal Motor Carrier Safety Administration (FMCSA)
  - Federal Highway Administration (FHWA)
  - Intelligent Transportation System Joint Program Office (ITS JPO)

© 2016 Productivity Apex, Inc.

Technologies Evaluated

- **Weigh in Motion (WIM) scales** – record axel weights and gross vehicle weights as trucks drive through a weigh station. There are both ramp and mainline WIMs
- **Kentucky Automatic Truck Screening (KATS)** – automated screening of trucks based on the license plate number and the USDOT number
- **Automated License Plate Reader (ALPR)** – captures license plate images and compares with safety databases
- **SRI Prototype (SRI Dashboard)** – integrated system to display WIM and static scale results and Safety and Fitness Electronic Records (SAFER) data to inspectors and drivers' mobile devices. This was developed the USDOT funded SRI Prototype Project
- **Other technologies at the test sites:**
  - **Static Scales**
  - **Infrared Cameras**
  - Pre-Clearance/Bypass Technologies: **PrePass; Drivewyze; NCPass**

© 2016 Productivity Apex, Inc.

Sites Evaluated

State: KENTUCKY

Main Technology: Kentucky Automatic Truck Screening (KATS)

Sites:

- Weigh Station at Lyon County



- Weigh Station at Simpson County



© 2016 Productivity Apex, Inc.

Sites Evaluated

State: **NORTH CAROLINA**

Main Technology: Weigh in Motion (WIM) scale and Automatic License Plate Reader (ALPR)

Sites:

- Mount Airy Weigh Station



© 2016 Productivity Apex, Inc.

Sites Evaluated

State: **MARYLAND & MICHIGAN**

Main Technology: SRI Prototype

Sites:

- West Friendship Weigh Station



- Grass Lake Weigh Station



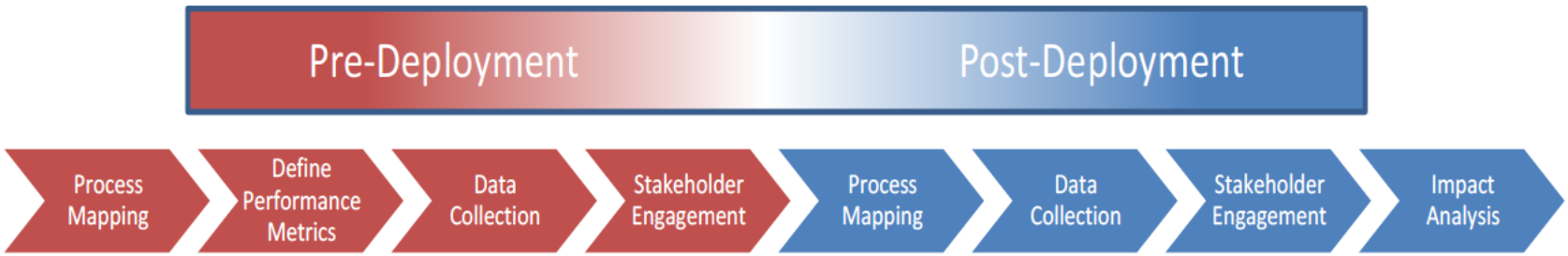
© 2016 Productivity Apex, Inc.

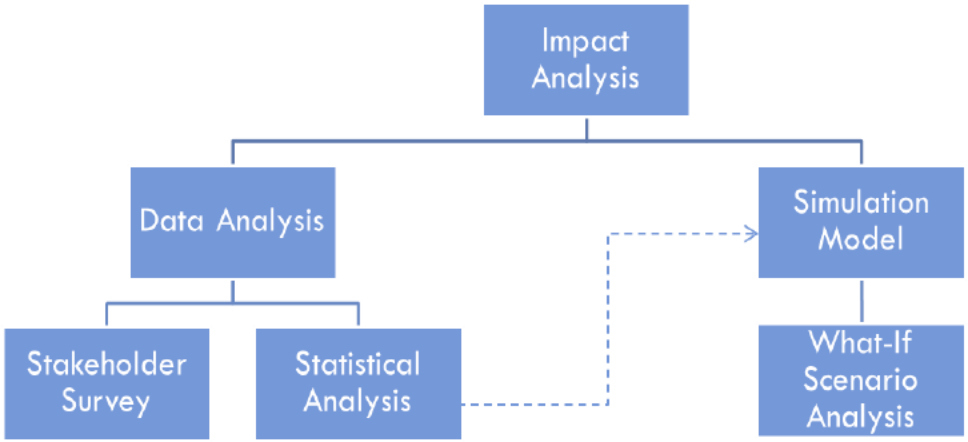
Impact Assessment Methodology

1. Collect pre- and post-deployment data for each site
2. Produce a sound analysis of the relative performance metrics for each site
3. Determine qualitative and quantitative impacts to the operations of inspection stations
4. Identify key attributes or characteristics to be considered when applying test site findings to a broader environment

© 2016 Productivity Apex, Inc.

Impact Assessment Methodology





© 2016 Productivity Apex, Inc.

Performance Measures

10

Goal	Performance Measures	Data	Quantitative/ Qualitative	Predominant Benefit
Increased Productive Inspections Time	Average proportion of time processing non-compliant vehicles (inspection and paperwork)	Inspection Duration, Inspection Start and End Time	Quantitative	Mobility; Agency Efficiency
		Inspection Duration, Inspection Start and End Time, Fuel Consumption Data, Emissions Data	Quantitative	Energy; Cost Savings
			Quantitative	Emissions
Increased Inspection Efficiency	Number of productive inspections per inspector (those with violations)	Inspections Results (Level I-V), Total Resources (Officers)	Quantitative	Agency Efficiency; Safety; Mobility
Increased Safety	Number of driver violations issued	Inspection Results (Level I-V)	Quantitative	Safety & Agency Efficiency
	Number of vehicle violations issued	Inspection Results (Level I-V)	Quantitative	Safety & Agency Efficiency
	Number of OOS assessments	Inspection Results (Level I-V), OOS counts	Quantitative	Safety & Agency Efficiency
User Acceptance	Number of satisfied users	Stakeholder Input	Qualitative	Agency Efficiency
Increased Revenue	Revenue generated through inspections	Financial metrics & historical data	Quantitative	Cost Benefit

Data Collection

- Data was collected from commercial vehicle enforcement agencies, state DOTS, and Pre-screening companies
- Pre- and Post- deployment data from each site (3 - 6 months)

Examples of data records collected:

- WIM and Static Scale daily counts
- Daily inspections, inspection level, duration, results, type of violation
- Out of Service violations, totals, and per driver and vehicle
- Traffic counts near site location
- Monthly revenue data and permits collected

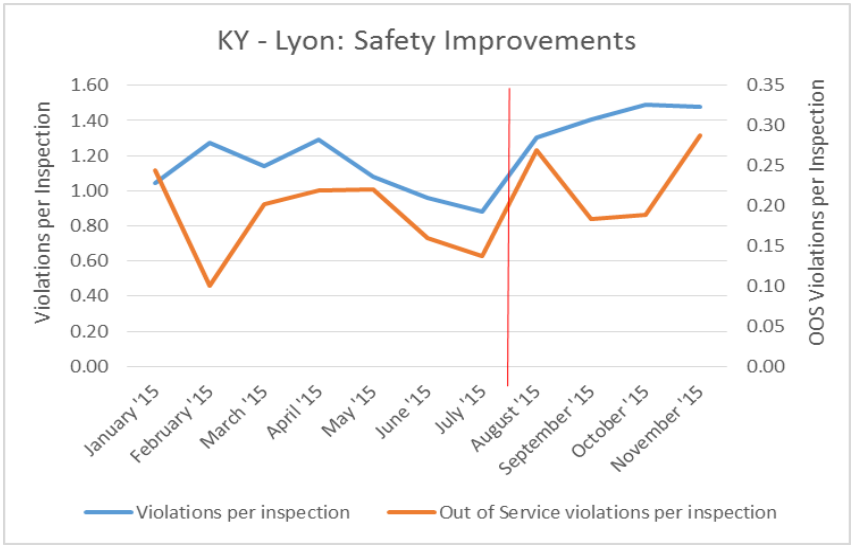
Used in:

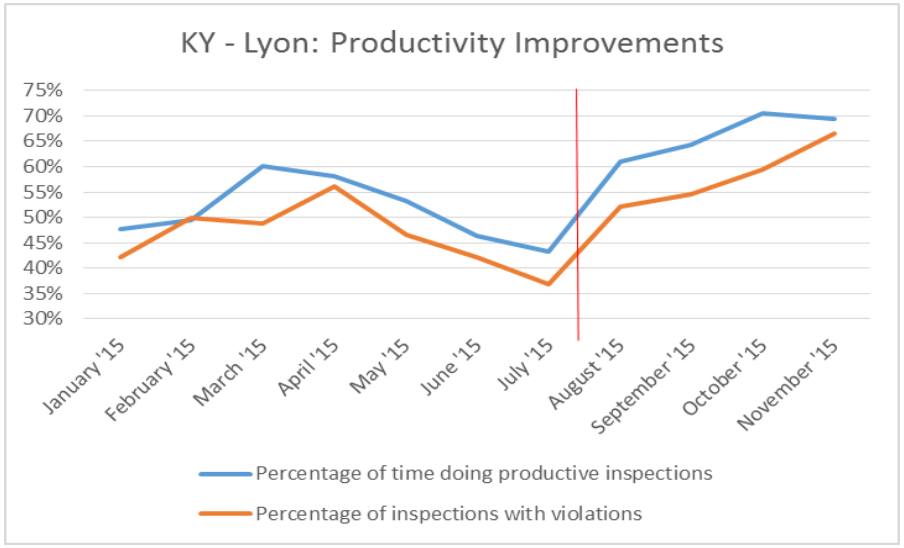
- Site Data Analysis
- Simulation Model

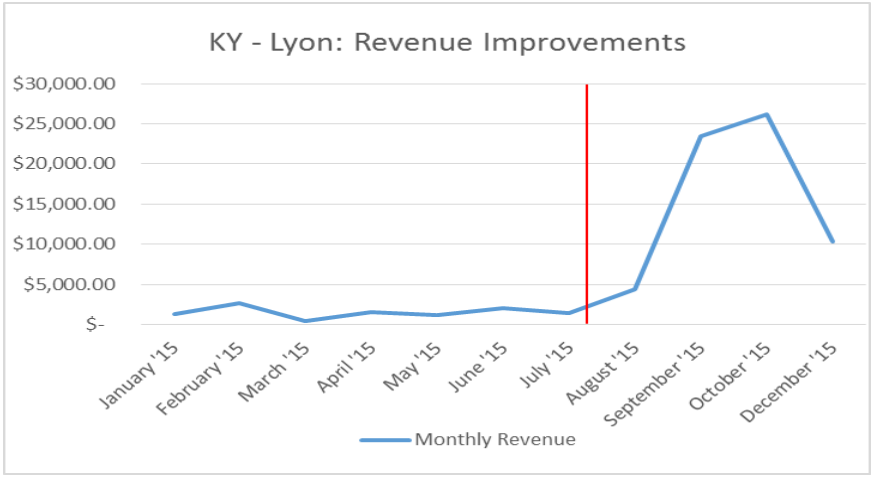
© 2016 Productivity Apex, Inc.

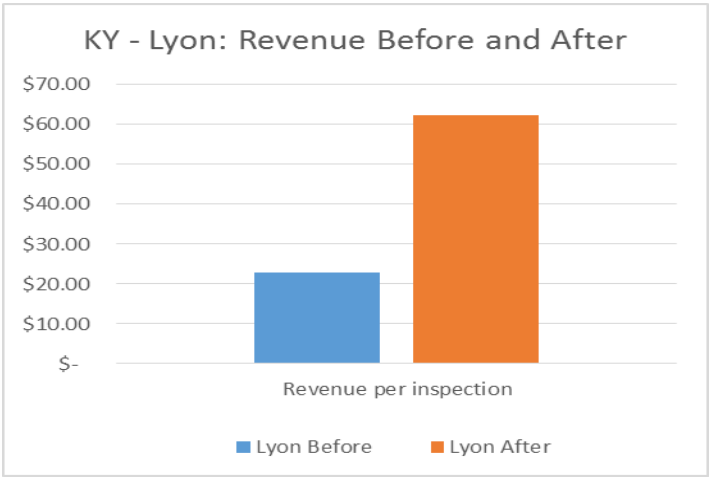
Data Analysis
Lyon, KY







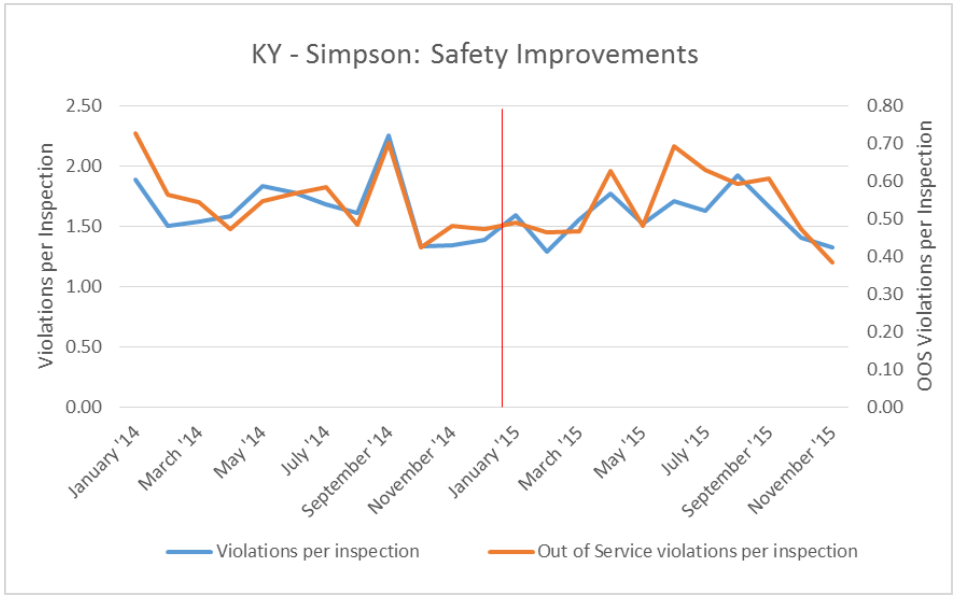


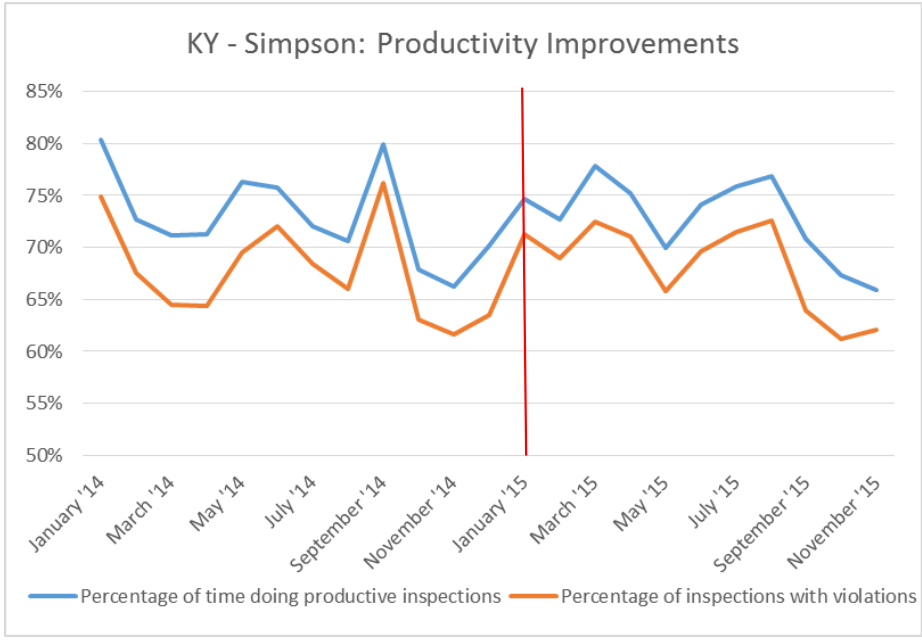


© 2016 Productivity Apex, Inc.

Data Analysis Simpson, KY



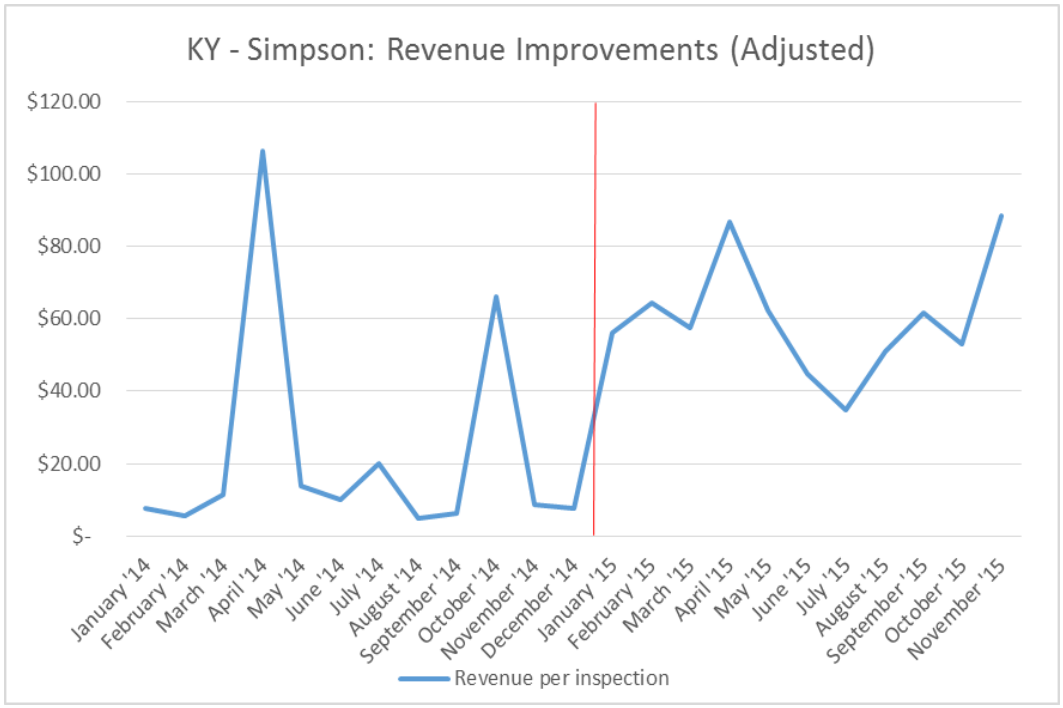


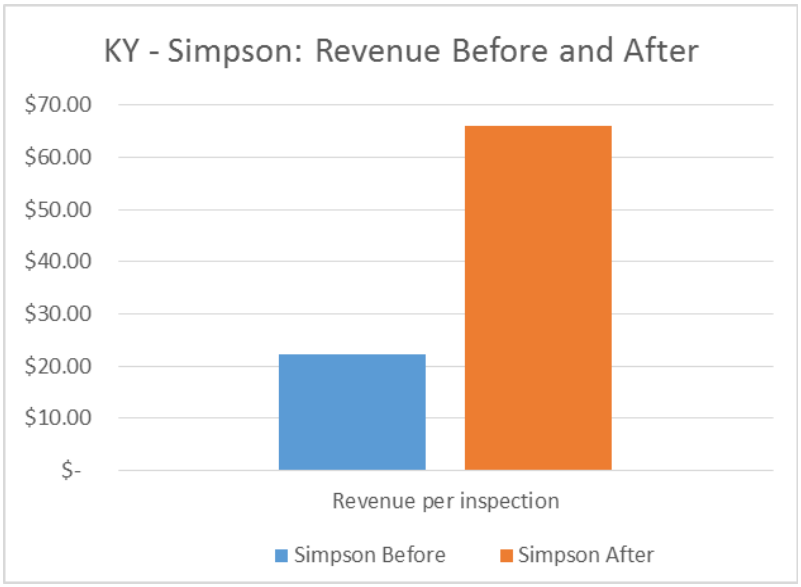


© 2016 Productivity Apex, Inc.

Simpson, KY (cont.)

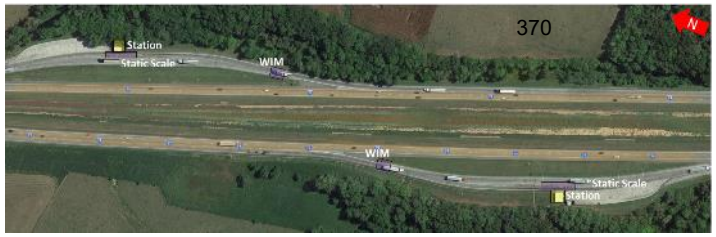


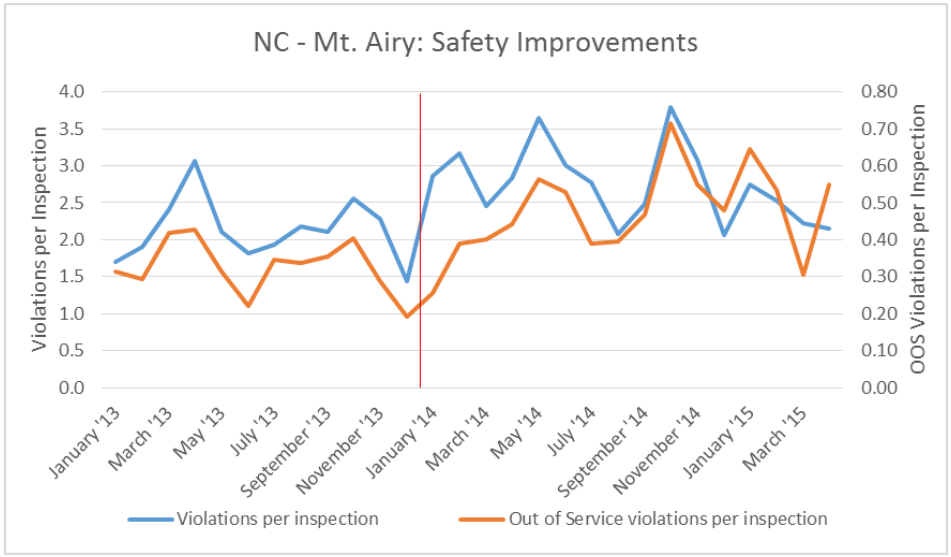


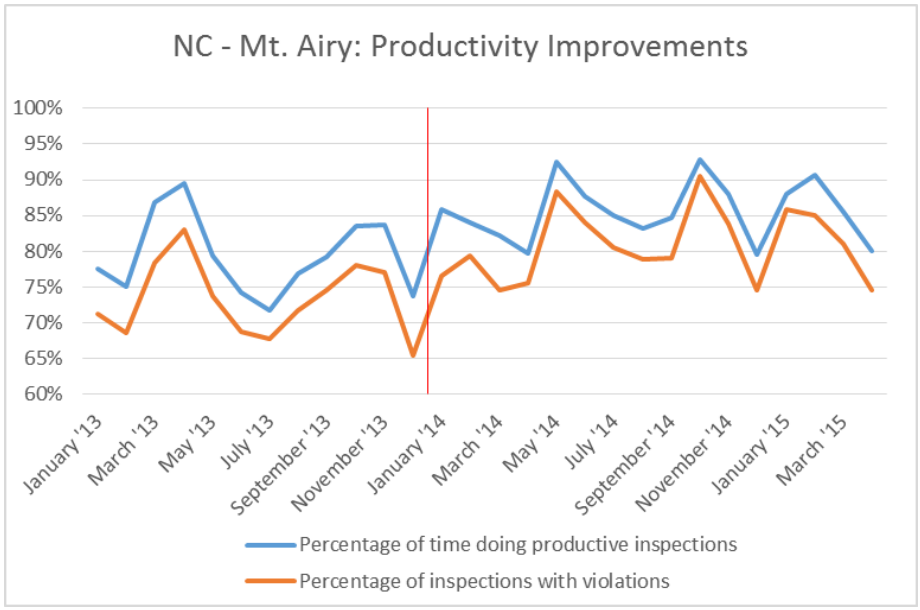


© 2016 Productivity Apex, Inc.

Data Analysis
Mt. Airy, NC

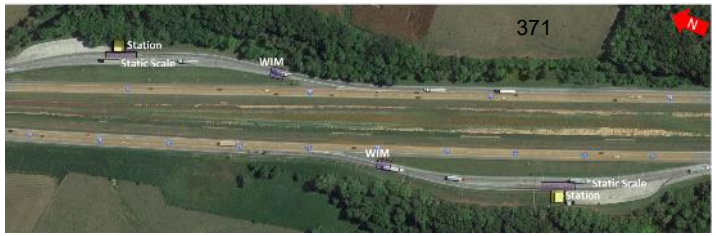


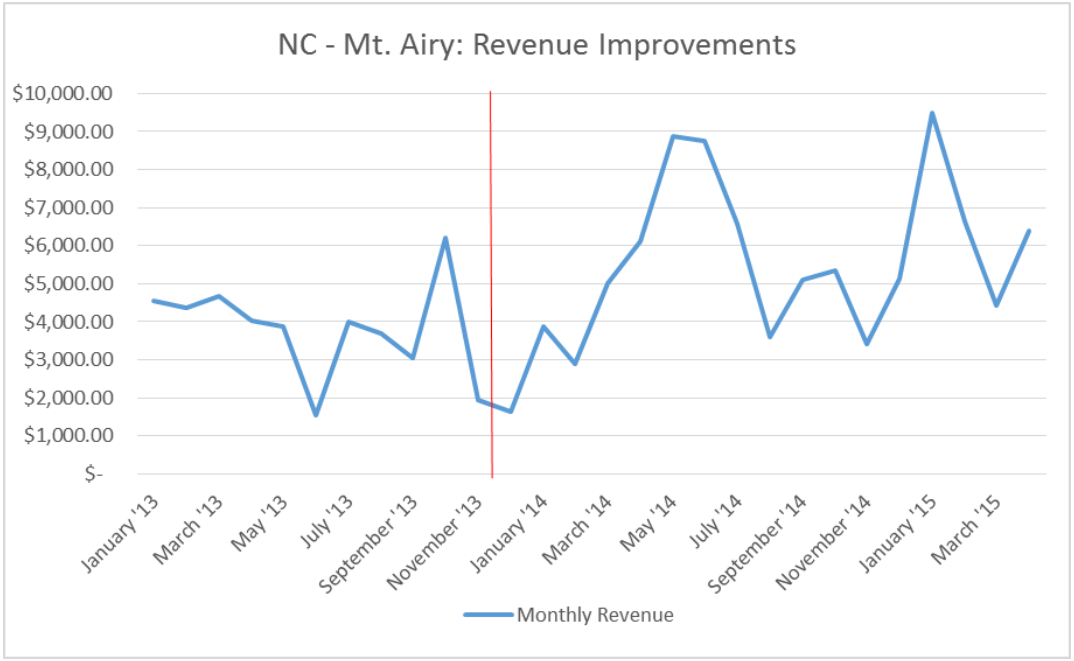


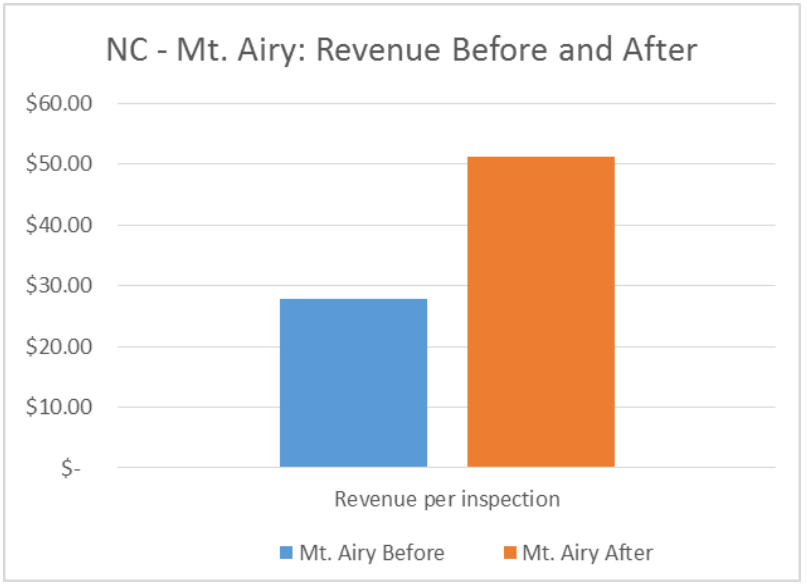


© 2016 Productivity Apex, Inc.

Mt. Airy, NC (cont.)







© 2016 Productivity Apex, Inc.

Stakeholder Surveys

Commercial Vehicle Enforcement Perception Survey

Kentucky – 20 Respondents

Questions	Yes		No	
Have you used the KATS system to perform commercial vehicle inspections?	94.74%		5.26%	
Have you noticed a change in driver behavior during inspections after implementing KATS?	15.79%		84.21%	
Do you thinks KATS has changed drivers' attitude towards inspections?	26.32%		73.68%	
	Improved	Not Improved	Made Worse	Don't Know
To what degree has KATS improved your ability to identify commercial vehicle violations?	100%	0%	0%	0%
	Positively	No Impact	Negatively	Don't Know
To what degree do you believe KATS has impacted the safety of individual truck drivers?	47.37%	31.58%	0%	21.05%
To what degree do you believe KATS has impacted safety conditions in this corridor?	57.90%	31.57%	0%	10.53%

© 2016 Productivity Apex, Inc.

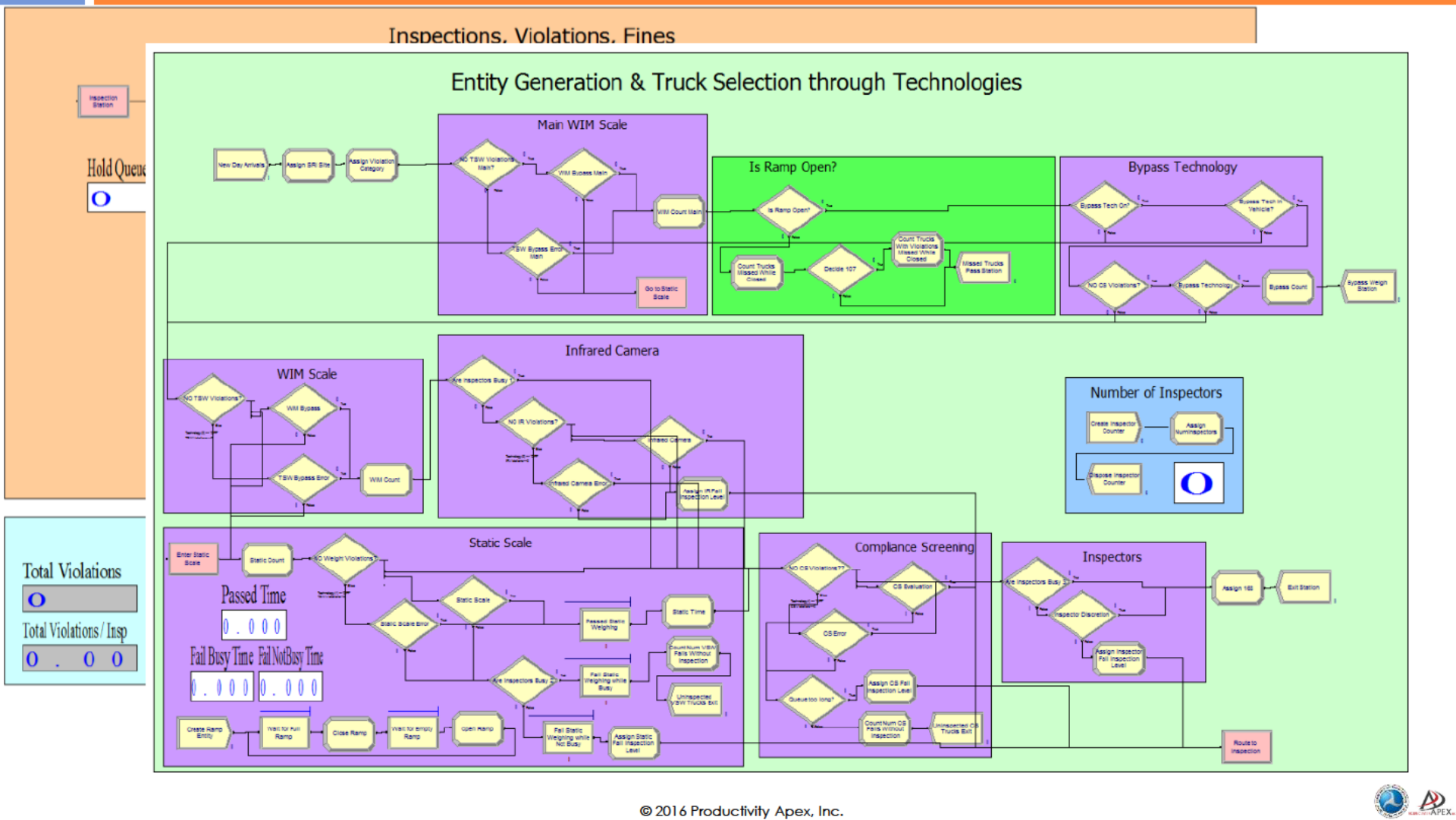
Simulation Objective

The following two main objectives were formulated for the development of this simulation model:

- To measure and compare the impact of deploying mainline and in-ramp technologies at a weigh station
- To analyze the effect of technology adoption by the user

© 2016 Productivity Apex, Inc.

Simulation Model



© 2016 Productivity Apex, Inc.

Model Assumptions and Data

- The technologies evaluated are 100% accurate and active
- The following systems and technologies are active in the model: mainline WIM, In-Ramp WIM, Static Scale, Compliance Screening system in the mainline (By-Passing technology), In-Ramp compliance screening system.
- Compliance screening technologies both in-ramp and in the mainline would have the same capability for detecting the same type of violations
- There are no vehicles pulled based on inspector discretion
- There is only one inspection pit on each site
- There is always 100% resource availability for inspections
- There is one static scale only at the site
- The site is in operations for 10 hours a day
- The probability of having a violation is based on an analysis of two years of inspection records from the Kentucky Lyon and Simpson sites

© 2016 Productivity Apex, Inc.

Simulation Analysis Scenarios & Results

Use Case #1: Impact of compliance screening technologies in-ramp and mainline

- Having a e-Screening systems in the mainline allows capturing almost the same number of violators compared to having similar systems on ramp in-ramp.
- However, helps to filter out vehicles with low probability of violations allowing them to bypass.
- This could increase the efficiency by making the inspections more productive
- Screening vehicles at highway speed minimize delays and improve efficiencies; hence, potentially reduce the environmental impact of commercial motor vehicles.

Use Case #2: Impact of technology adoption for bypassing technology and random pull levels

- Impact of changing the random pull levels is directly proportional to the adoption rate of the technology.
- Increasing the technology adoption rates would bring the most benefits in productivity and efficiency.
- The variation of random pull levels didn't have a major impact on the number of vehicles found with violations.
- There could be a bigger impact in number of vehicles found violations if technology could detect mechanical or visual issues

© 2016 Productivity Apex, Inc.

Conclusion (From In-progress Analysis)

- **Pre & Post Deployment Data Analysis:**
  - Technologies improved productivity, effectiveness, and efficiency
  - The analyses showed that e-screening technologies increased the number of out of service violations detected at enforcement sites
  - The increased revenue observed in all sites where these technologies were deployed was unexpected
- **Surveys:**
  - All respondents agree that SRI like technologies improved the ability to identify commercial vehicle violations
- **Simulation:**
  - Mainline system benefits drivers and enforcement by reducing delays for drivers and improving the productivity at the station
  - Bigger benefits are achieved by increasing the technologies adoption rate

© 2016 Productivity Apex, Inc.

Quote 3000000793710.1
MA-EXEC OFFICE PUBLIC SAFETY

Salesperson

Salesperson Name
Alex Brooks

Salesperson Email
Alex_Brooks@Dell.com

Salesperson Phone
1(800) 456-3355

Salesperson Extension
5138305

Quote Details

Quote Date
10/04/2016

Quote Validity
11/03/2016

Solution ID
-

Billing Details

Company Name
MA-EXEC OFFICE PUBLIC SAFETY

Customer Number
98596528

Phone Number
1 (617) 7276950

Address
1 ASHBURTON PL RM 2133
BOSTON
MA
02108-1518
US

Price Summary

Description	Quantity	Unit Price	Subtotal Price
PowerEdge R730	1	$13,755.12	$13,755.12
		Subtotal	$13,755.12
		*Taxable Amount	$0.00
		*Non-Taxable Amount	$13,755.12
		Tax	$0.00
		Shipping and Handling	$0.00
		Environmental Fee	$0.00
		Total	**$13,755.12**

Note: All tax quoted above is an estimate; final taxes will be listed on the invoice.

© 2014 Dell Inc. U.S. only. Dell Inc. is located at One Dell Way, Mail Stop 8129, Round Rock, TX 78682.

Dear Customer,

Please review the quote for product and information accuracy.
If you find errors or desire changes, please contact me as soon as possible.

Regards,
Alex Brooks

Order this quote easily online through your Premier page, or if you do not have Premier, using Quote to Order

Product Details by Shipment

Shipping Group 1

Shipping Contact:	SEAN HUGHES
Shipping Phone No:	1 (617) 6604620
Shipping via:	Standard Ground
Shipping Address:	200 ARLINGTON ST CHELSEA MA 02150-2375 US

Subtotal	$13,755.12
Tax	$0.00
Shipping and Handling	$0.00
Environmental Fee	$0.00
Total	$13,755.12

Description	Quantity	Unit Price	Subtotal Price
PowerEdge R730	1	$13,755.12	$13,755.12

Estimated Delivery Date: 10/14/2016
Contract Code: 78AFH
Customer Agreement No: ITC47

210-ACXU	PowerEdge R730 Server	1	-	-
329-BCZK	PE R730/xd Motherboard MLK	1	-	-
461-AADZ	No Trusted Platform Module	1	-	-
350-BBEN	Chassis with up to 8, 2.5" Hard Drives	1	-	-
340-AKKB	PowerEdge R730 Shipping	1	-	-
338-BJDU	Intel Xeon E5-2637 v4 3.5GHz,15M Cache,9.60GT/s QPI,Turbo,HT,4C/8T (135W) Max Mem 2400MHz	1	-	-
338-BJEG	Intel Xeon E5-2637 v4 3.5GHz,15M Cache,9.60GT/s QPI,Turbo,HT,4C/8T (135W) Max Mem 2400MHz	1	-	-
370-ABWE	DIMM Blanks for System with 2 Processors	1	-	-
374-BBHM	Standard Heatsink for PowerEdge R730/R730xd	1	-	-
374-BBHM	Standard Heatsink for PowerEdge R730/R730xd	1	-	-
370-ACPH	2400MT/s RDIMMs	1	-	-
370-AAIP	Performance Optimized	1	-	-
780-BBJV	RAID 5 for H330/H730/H730P (3-16 HDDs or SSDs)	1	-	-

© 2014 Dell Inc. U.S. only. Dell Inc. is located at One Dell Way, Mail Stop 8129, Round Rock, TX 78682.

405-AAEH	PERC H730P Integrated RAID Controller, 2GB Cache	1	-	-
540-BBBW	Broadcom 5720 QP 1Gb Network Daughter Card	1	-	-
385-BBHO	iDRAC8 Enterprise, integrated Dell Remote Access Controller, Enterprise	1	-	-
429-AAPU	DVD ROM, SATA, INTERNAL	1	-	-
350-BBEJ	Bezel	1	-	-
770-BBBQ	ReadyRails Sliding Rails Without Cable Management Arm	1	-	-
384-BBBL	Performance BIOS Settings	1	-	-
450-ADWM	Dual, Hot-plug, Redundant Power Supply (1+1), 1100W	1	-	-
631-AAJG	Electronic System Documentation and OpenManage DVD Kit, PowerEdge R730/xd	1	-	-
618-BBDS	Windows Server 2012R2 Standard Edition,Factory Installed, No Media, 2 Socket, 2 VMs,NO CALs	1	-	-
634-BBOZ	Windows Server 2012R2 Standard, Media, FI Standard Ed Downgrade image, Eng	1	-	-
332-1286	US Order	1	-	-
330-BBCO	R730/xd PCIe Riser 2, Center	1	-	-
330-BBCP	R730 PCIe Riser 3, Left Alternate	1	-	-
330-BBCR	R730/xd PCIe Riser 1, Right	1	-	-
976-8706	Dell Hardware Limited Warranty Plus On Site Service	1	-	-
976-8709	MISSION CRITICAL PACKAGE: Enhanced Services, 3 Year	1	-	-
976-8710	Mission Critical Package: 4-Hour 7x24 On-Site Service with Emergency Dispatch, 3 Year	1	-	-
976-8711	ProSupport: 7x24 HW / SW Tech Support and Assistance, 3 Year	1	-	-
989-3439	Thank you choosing Dell ProSupport. For tech support, visit http://www.dell.com/support or call 1-800- 945-3355	1	-	-
900-9997	On-Site Installation Declined	1	-	-
973-2426	Declined Remote Consulting Service	1	-	-
983-6402	Keep Your Hard Drive, 3 Year	1	-	-
370-ACNS	32GB RDIMM, 2400MT/s, Dual Rank, x4 Data Width	8	-	-
400-AIFQ	800GB Solid State Drive SATA Mix Use MLC 6Gpbs 2.5in Hot-plug Drive, S3610	7	-	-
540-BBRO	Intel X550 Dual Port 10G Base-T Adapter, Full Height	2	-	-
492-BBDH	C13 to C14, PDU Style, 12 AMP, 2 Feet (.6m) Power Cord, North America	2	-	-
492-BBDI	C13 to C14, PDU Style, 12 AMP, 6.5 Feet (2m) Power Cord, North America	2	-	-

© 2014 Dell Inc. U.S. only. Dell Inc. is located at One Dell Way, Mail Stop 8129, Round Rock, TX 78682.

Important Notes

Terms of Sale

This quote is valid for 30 days unless otherwise stated. Unless you have a separate written agreement with Dell that specifically applies to this order, your order will be subject to and governed by the following agreements, each of which are incorporated herein by reference and available in hardcopy from Dell at your request:

If this purchase is for your internal use only: Dell's Commercial Terms of Sale (http://www.dell.com/CTS), which incorporate Dell's U.S. Return Policy (www.dell.com/returnpolicy) and Warranty (www.dell.com/warrantyterms).

If this purchase is intended for resale: Dell's Reseller Terms of Sale (www.dell.com/resellerterms).

If this purchase includes services: in addition to the foregoing applicable terms, Dell's service contracts and related service terms (www.dell.com/servicecontracts/global).

If this purchase includes software: in addition to the foregoing applicable terms, your use of the software is subject to the license terms accompanying the software, and in the absence of such terms, then use of the Dell-branded application software is subject to the Dell End User License Agreement - A Version (www.dell.com/AEULA) and use of the Dell-branded system software is subject to the Dell End User License Agreement - S Version (www.dell.com/SEULA).

You acknowledge having read and agree to be bound by the foregoing applicable terms in their entirety. Any terms and conditions set forth in your purchase order or any other correspondence that are in addition to, inconsistent or in conflict with, the foregoing applicable online terms will be of no force or effect unless specifically agreed to in a writing signed by Dell that expressly references such terms.

Pricing, Taxes, and Additional Information

All product, pricing, and other information is valid for U.S. customers and U.S. addresses only, and is based on the latest information available and may be subject to change. Dell reserves the right to cancel quotes and orders arising from pricing or other errors. Please indicate any tax-exempt status on your PO, and fax your exemption certificate, including your Customer Number, to the Dell Tax Department at 800-433-9023. Please ensure that your tax-exemption certificate reflects the correct Dell entity name: **Dell Marketing L.P.** Note: All tax quoted above is an estimate; final taxes will be listed on the invoice. If you have any questions regarding tax please send an e-mail to Tax_Department@dell.com.

For certain products shipped to end-users in California, a State Environmental Fee will be applied to your invoice. Dell encourages customers to dispose of electronic equipment properly.

© 2014 Dell Inc. U.S. only. Dell Inc. is located at One Dell Way, Mail Stop 8129, Round Rock, TX 78682.

Quote 3000000792939.1
MA-EXEC OFFICE PUBLIC SAFETY

Salesperson

Salesperson Name
Alex Brooks

Salesperson Email
Alex_Brooks@Dell.com

Salesperson Phone
1(800) 456-3355

Salesperson Extension
5138305

Quote Details

Quote Date
10/04/2016

Quote Validity
11/03/2016

Solution ID
-

Billing Details

Company Name
MA-EXEC OFFICE PUBLIC SAFETY

Customer Number
98596528

Phone Number
1 (617) 7276950

Address
1 ASHBURTON PL RM 2133
BOSTON
MA
02108-1518
US

Price Summary

Description	Quantity	Unit Price	Subtotal Price
PowerEdge R730	1	$15,610.65	$15,610.65
		Subtotal	$15,610.65
		*Taxable Amount	$0.00
		*Non-Taxable Amount	$15,610.65
		Tax	$0.00
		Shipping and Handling	$0.00
		Environmental Fee	$0.00
		Total	**$15,610.65**

Note: All tax quoted above is an estimate; final taxes will be listed on the invoice.

© 2014 Dell Inc. U.S. only. Dell Inc. is located at One Dell Way, Mail Stop 8129, Round Rock, TX 78682.

Dear Customer,

Please review the quote for product and information accuracy.
If you find errors or desire changes, please contact me as soon as possible.

Regards,
Alex Brooks

Order this quote easily online through your Premier page, or if you do not have Premier, using Quote to Order

Product Details by Shipment

Shipping Group 1

Shipping Contact:	SEAN HUGHES
Shipping Phone No:	1 (617) 6604620
Shipping via:	Standard Ground
Shipping Address:	200 ARLINGTON ST CHELSEA MA 02150-2375 US

Subtotal	$15,610.65
Tax	$0.00
Shipping and Handling	$0.00
Environmental Fee	$0.00
Total	$15,610.65

Description	Quantity	Unit Price	Subtotal Price
PowerEdge R730	1	$15,610.65	$15,610.65

Estimated Delivery Date: 12/30/2016
Contract Code: 78AFH
Customer Agreement No: ITC47

210-ACXU	PowerEdge R730 Server	1	-	-
329-BCZK	PE R730/xd Motherboard MLK	1	-	-
461-AADZ	No Trusted Platform Module	1	-	-
350-BBEN	Chassis with up to 8, 2.5" Hard Drives	1	-	-
340-AKKB	PowerEdge R730 Shipping	1	-	-
338-BJDU	Intel Xeon E5-2637 v4 3.5GHz,15M Cache,9.60GT/s QPI,Turbo,HT,4C/8T (135W) Max Mem 2400MHz	1	-	-
338-BJEG	Intel Xeon E5-2637 v4 3.5GHz,15M Cache,9.60GT/s QPI,Turbo,HT,4C/8T (135W) Max Mem 2400MHz	1	-	-
370-ABWE	DIMM Blanks for System with 2 Processors	1	-	-
374-BBHM	Standard Heatsink for PowerEdge R730/R730xd	1	-	-
374-BBHM	Standard Heatsink for PowerEdge R730/R730xd	1	-	-
370-ACPH	2400MT/s RDIMMs	1	-	-
370-AAIP	Performance Optimized	1	-	-
780-BBJV	RAID 5 for H330/H730/H730P (3-16 HDDs or SSDs)	1	-	-

© 2014 Dell Inc. U.S. only. Dell Inc. is located at One Dell Way, Mail Stop 8129, Round Rock, TX 78682.

405-AAEH	PERC H730P Integrated RAID Controller, 2GB Cache	1	-	-
540-BBBW	Broadcom 5720 QP 1Gb Network Daughter Card	1	-	-
385-BBHO	iDRAC8 Enterprise, integrated Dell Remote Access Controller, Enterprise	1	-	-
429-AAPU	DVD ROM, SATA, INTERNAL	1	-	-
350-BBEJ	Bezel	1	-	-
770-BBBQ	ReadyRails Sliding Rails Without Cable Management Arm	1	-	-
384-BBBL	Performance BIOS Settings	1	-	-
450-ADWM	Dual, Hot-plug, Redundant Power Supply (1+1), 1100W	1	-	-
631-AAJG	Electronic System Documentation and OpenManage DVD Kit, PowerEdge R730/xd	1	-	-
618-BBDS	Windows Server 2012R2 Standard Edition,Factory Installed, No Media, 2 Socket, 2 VMs,NO CALs	1	-	-
634-BBOZ	Windows Server 2012R2 Standard, Media, FI Standard Ed Downgrade image, Eng	1	-	-
332-1286	US Order	1	-	-
330-BBCO	R730/xd PCIe Riser 2, Center	1	-	-
330-BBCP	R730 PCIe Riser 3, Left Alternate	1	-	-
330-BBCR	R730/xd PCIe Riser 1, Right	1	-	-
976-8706	Dell Hardware Limited Warranty Plus On Site Service	1	-	-
976-8709	MISSION CRITICAL PACKAGE: Enhanced Services, 3 Year	1	-	-
976-8710	Mission Critical Package: 4-Hour 7x24 On-Site Service with Emergency Dispatch, 3 Year	1	-	-
976-8711	ProSupport: 7x24 HW / SW Tech Support and Assistance, 3 Year	1	-	-
989-3439	Thank you choosing Dell ProSupport. For tech support, visit http://www.dell.com/support or call 1-800- 945-3355	1	-	-
900-9997	On-Site Installation Declined	1	-	-
973-2426	Declined Remote Consulting Service	1	-	-
983-6402	Keep Your Hard Drive, 3 Year	1	-	-
370-ACNX	16GB RDIMM, 2400MT/s, Dual Rank, x8 Data Width	8	-	-
400-ANNT	960GB Solid State Drive SAS Mix Use MLC 12Gbps 2.5in Hot-plug Drive, PX04SV	8	-	-
540-BBRO	Intel X550 Dual Port 10G Base-T Adapter, Full Height	2	-	-
492-BBDH	C13 to C14, PDU Style, 12 AMP, 2 Feet (.6m) Power Cord, North America	2	-	-
492-BBDI	C13 to C14, PDU Style, 12 AMP, 6.5 Feet (2m) Power Cord, North America	2	-	-

© 2014 Dell Inc. U.S. only. Dell Inc. is located at One Dell Way, Mail Stop 8129, Round Rock, TX 78682.

Important Notes

Terms of Sale

This quote is valid for 30 days unless otherwise stated. Unless you have a separate written agreement with Dell that specifically applies to this order, your order will be subject to and governed by the following agreements, each of which are incorporated herein by reference and available in hardcopy from Dell at your request:

If this purchase is for your internal use only: Dell's Commercial Terms of Sale (http://www.dell.com/CTS), which incorporate Dell's U.S. Return Policy (www.dell.com/returnpolicy) and Warranty (www.dell.com/warrantyterms).

If this purchase is intended for resale: Dell's Reseller Terms of Sale (www.dell.com/resellerterms).

If this purchase includes services: in addition to the foregoing applicable terms, Dell's service contracts and related service terms (www.dell.com/servicecontracts/global).

If this purchase includes software: in addition to the foregoing applicable terms, your use of the software is subject to the license terms accompanying the software, and in the absence of such terms, then use of the Dell-branded application software is subject to the Dell End User License Agreement - A Version (www.dell.com/AEULA) and use of the Dell-branded system software is subject to the Dell End User License Agreement - S Version (www.dell.com/SEULA).

You acknowledge having read and agree to be bound by the foregoing applicable terms in their entirety. Any terms and conditions set forth in your purchase order or any other correspondence that are in addition to, inconsistent or in conflict with, the foregoing applicable online terms will be of no force or effect unless specifically agreed to in a writing signed by Dell that expressly references such terms.

Pricing, Taxes, and Additional Information

All product, pricing, and other information is valid for U.S. customers and U.S. addresses only, and is based on the latest information available and may be subject to change. Dell reserves the right to cancel quotes and orders arising from pricing or other errors. Please indicate any tax-exempt status on your PO, and fax your exemption certificate, including your Customer Number, to the Dell Tax Department at 800-433-9023. Please ensure that your tax-exemption certificate reflects the correct Dell entity name: **Dell Marketing L.P.** Note: All tax quoted above is an estimate; final taxes will be listed on the invoice. If you have any questions regarding tax please send an e-mail to Tax_Department@dell.com.

For certain products shipped to end-users in California, a State Environmental Fee will be applied to your invoice. Dell encourages customers to dispose of electronic equipment properly.

© 2014 Dell Inc. U.S. only. Dell Inc. is located at One Dell Way, Mail Stop 8129, Round Rock, TX 78682.

Directions

Connecticut Academy of Science and Engineering (CASE)
Located at the
Connecticut Economic Resource Center (CERC)

805 Brook Street, Rocky Hill, CT

Directions

From Hartford, Bradley Airport and Points North

- Take I-91 South to Exit 23
- Turn right at end of ramp onto West Street
- Continue to T-shaped intersection (West Street & Route 3)
- Turn left onto Route 3
- Turn left at 3rd traffic light onto Brook Street
- Turn left into first driveway (I-91 Tech Center)
- CASE/CERC are in Building #4

From New Haven, Middletown and Points South

- Take I-91 North to Exit 23
- Turn left at end of ramp onto West Street
- Continue to T-shaped intersection (West Street & Route 3)
- Turn left onto Route 3
- Turn left at 3rd traffic light onto Brook Street
- Turn left into first driveway (I-91 Tech Center)
- CASE/CERC are in Building #4

From Waterbury, Danbury and Points West

- Take I-84 East to Exit 27, I-691 East
- Take Exit 11 to I-91 North
- Take I-91 North to Exit 23
- Turn left at end of ramp onto West Street
- Continue to T-shaped intersection (West Street & Route 3)
- Turn left onto Route 3
- Turn left at 3rd traffic light onto Brook Street
- Turn left into first driveway (I-91 Tech Center)
- CASE/CERC are in Building #4

EOPSS Remote Access VPN
Client and Certificate Installation

Table of Contents

Client Retrieval 2
Client Unpacking 2
Manual Old Client Removal 3
Old Client Removal 4
Client Installation 6
Personal Certificate Installation 7
Manual Client Installation 10
Manual Export of Personal Certificate for Backup purposes or for use on another device 14
Manual Import of Previously Exported Personal Certificate 17
How to use the EOPSS Remote Access Client. 19
Connecting: 19
Disconnecting: 20

Prepared by the Massachusetts Executive Office of Public Safety and Security's
Office of Technology and Information Services
Enterprise and Field Services Support Division

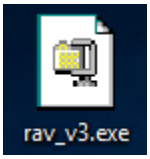
Last Updated: January 16, 2024

Client Retrieval

From a command prompt:
Type ***cd *** and enter
Type ***md vpn*** and enter
Type ***cd vpn*** and enter
type ***ftp cjisftp.chs.state.ma.us*** and enter
Type the username ***vpn*** and enter
Type the password ***vpn@OT1S*** and enter
Type ***bin*** and enter
Type ***get rav_v3.exe*** and enter
Type ***bye*** and enter

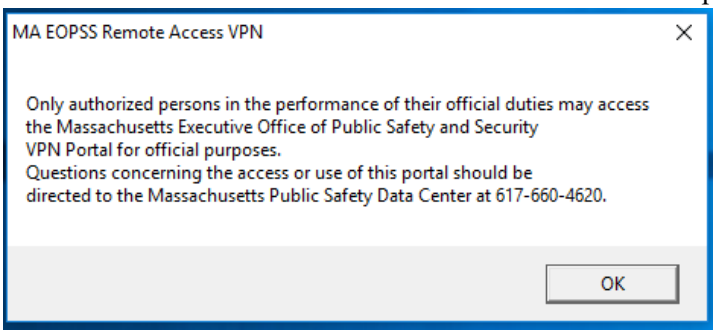
Client Unpacking

Move the **rav_v3.exe** file to the desktop.
Double click on the **rav_v3.exe** icon

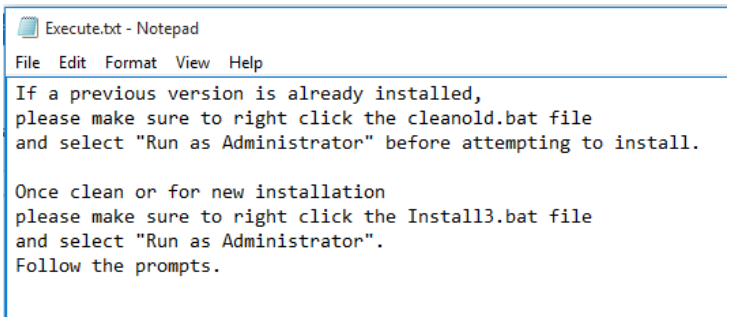


If prompted by Windows, **Click Yes to allow rav_v3.exe** to run

Click **Ok** in the "MA EOPSS Remote Access VPN"/WinZip Self-Extractor box

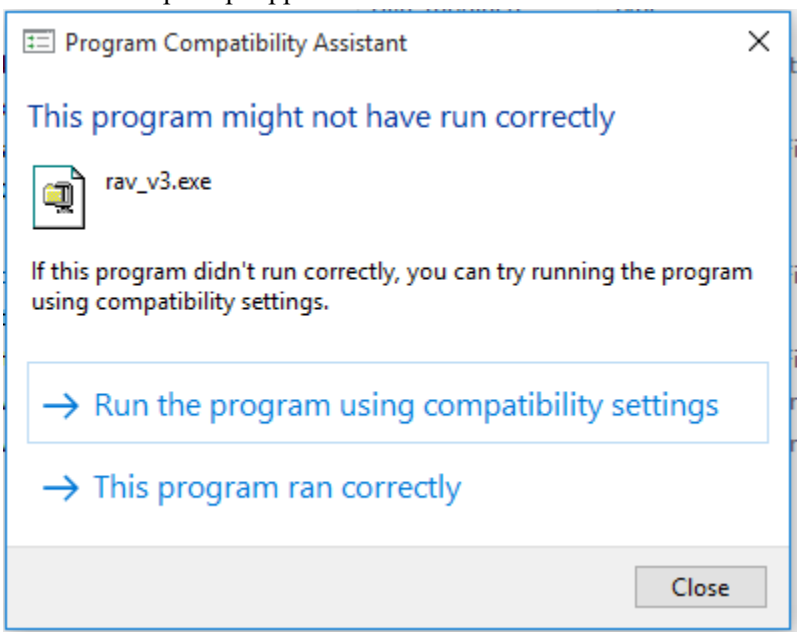


Several boxes will appear, please read the "Execute.txt notepad" file for installation instructions.



You may close the notepad file after reading.

If a windows prompt appears like below:



Select “This program ran correctly”.

Manual Old Client Removal

Prior to installing, please remove any previous versions of the client from Control Panel\All Control Panel Items\Programs and Features.

*** Note – If no previous client was installed, proceed to “Client Installation” ***

Also remove the below folders from the PC if they are not removed during uninstall:

C:\Program Files\Juniper Networks

C:\Users\Public\Juniper Networks

C:\Users\<username>\AppData\Roaming\Juniper Networks

C:\Program Files (x86)\Common Files\Juniper Networks

C:\Program Files (x86)\MA CJIS VPN

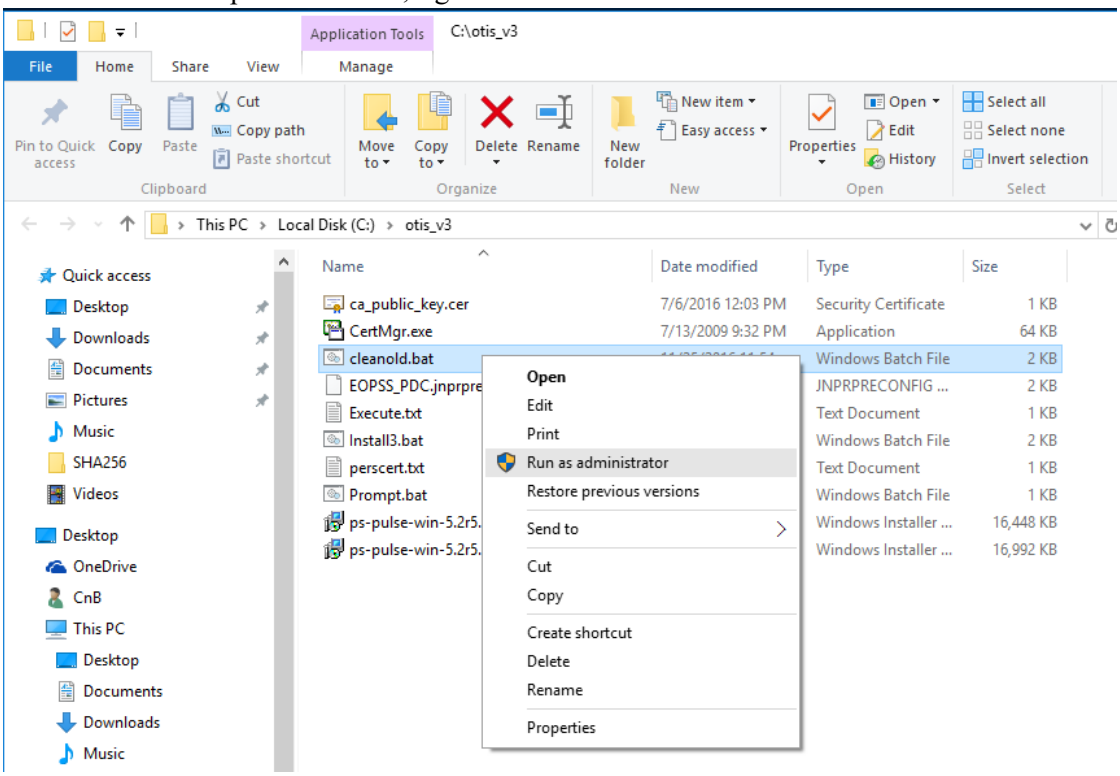
Searching the windows registry for all references to Juniper may be necessary.

The PC may restart automatically to complete the uninstallation, if it does NOT please initiate a restart before proceeding to the install.

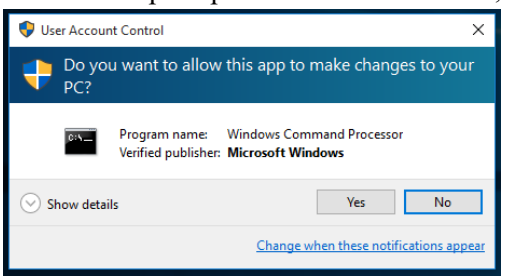
Old Client Removal

****If there was a client previously installed**,

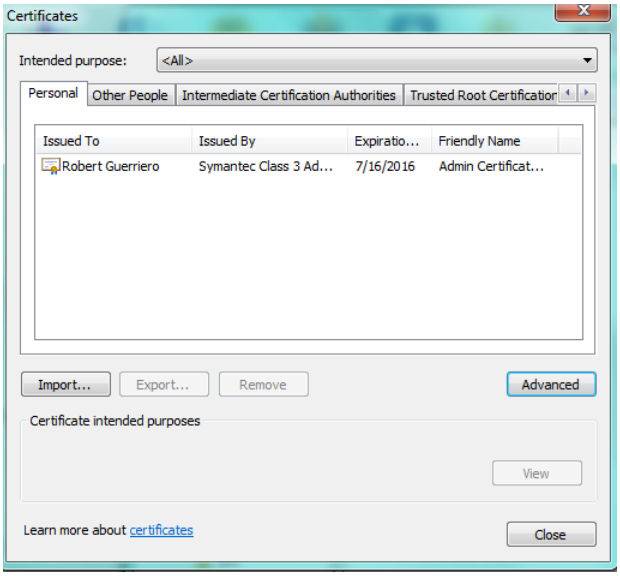
In the Windows Explorer window, right click on the **cleanold.bat** file and select “Run as administrator”:



You will be prompted with the below box, click **Yes**:



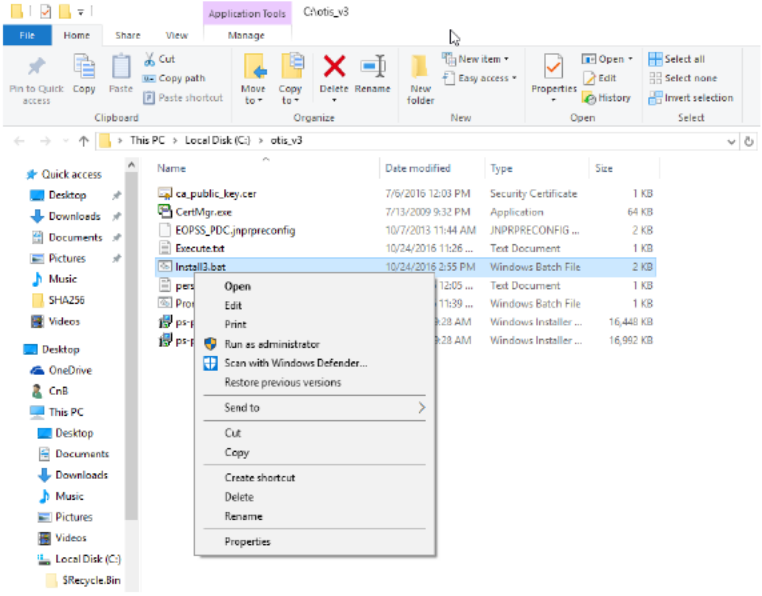
Another text file will appear, instructing you to remove the old personal certificate, in addition to a box labelled Certificates where the old personal certificate needs to be deleted. Select the name of the person's certificate on the "Personal" Tab, then click **Remove** and then **Close**.



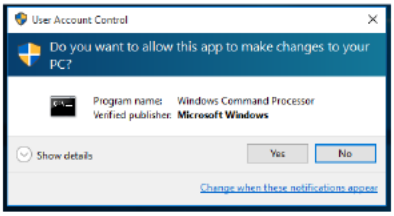
The PC may restart automatically to complete the uninstallation, if it does NOT please initiate a restart before proceeding to the install.

Client Installation

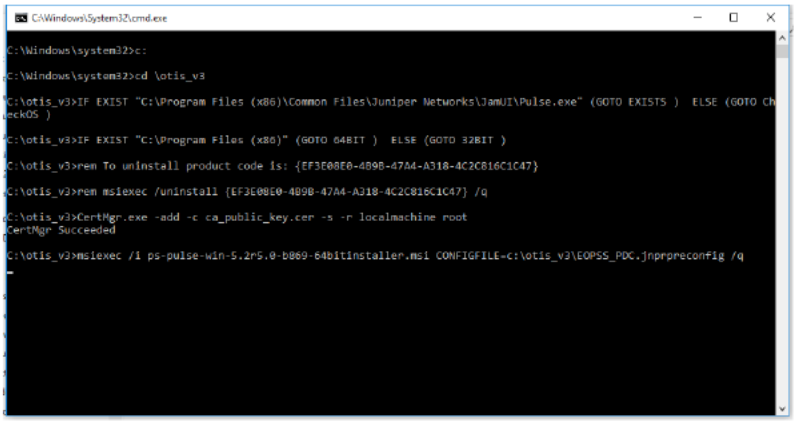
In the Windows Explorer window, navigate to "*C:\otis_v3*" and right click on the **install3.bat** file and select "Run as administrator":



You will be prompted with the below box, click **Yes**:



The following screen will appear for several minutes while the client install in the background.



Once completed the CMD/DOS window will disappear

Pulse icon will appear in the PC's tray



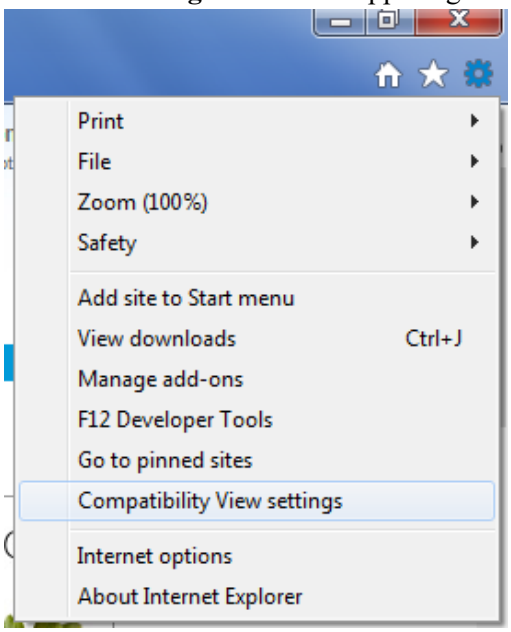
This completes the installation of the client, please proceed to personal certificate installation.

Personal Certificate Installation

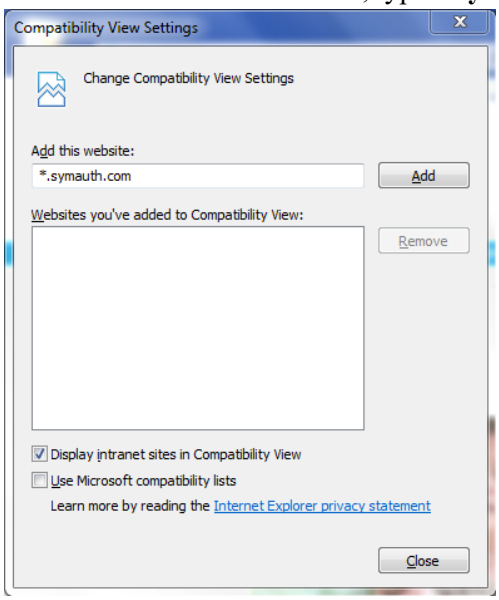
Open Internet Explorer, (do *NOT* use any other browser as the certificate will not get stored properly)
NOTE - ONLY IE 8, 9 10 OR 11 ARE SUPPORTED.

FOR IE11 ONLY, FOLLOW THE STEPS BELOW, OTHERWISE SKIP TO THE NEXT PAGE THAT BEGINS WITH PASTING THE ENROLLMENT CODE:

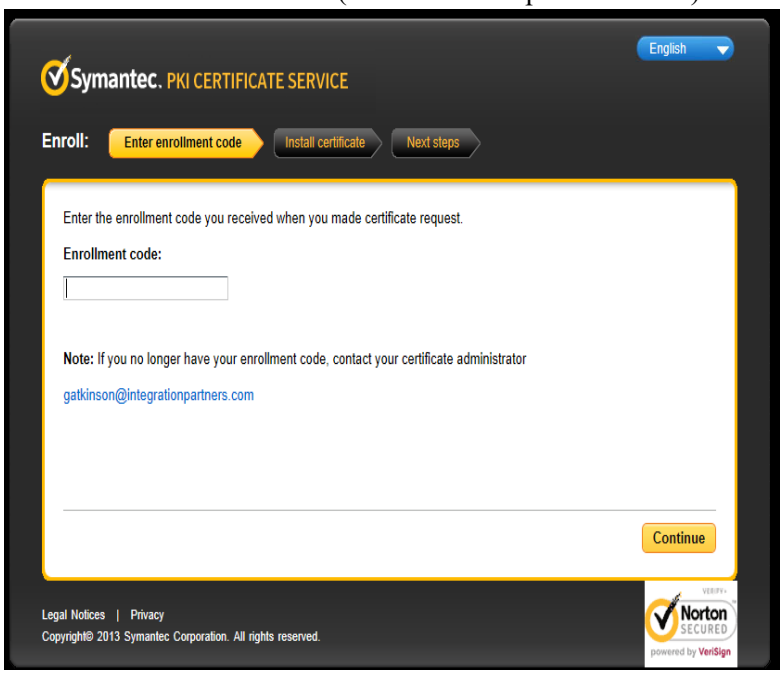
Click the **Settings** Icon in the upper right hand side, then click "**Compatibility View Settings**"



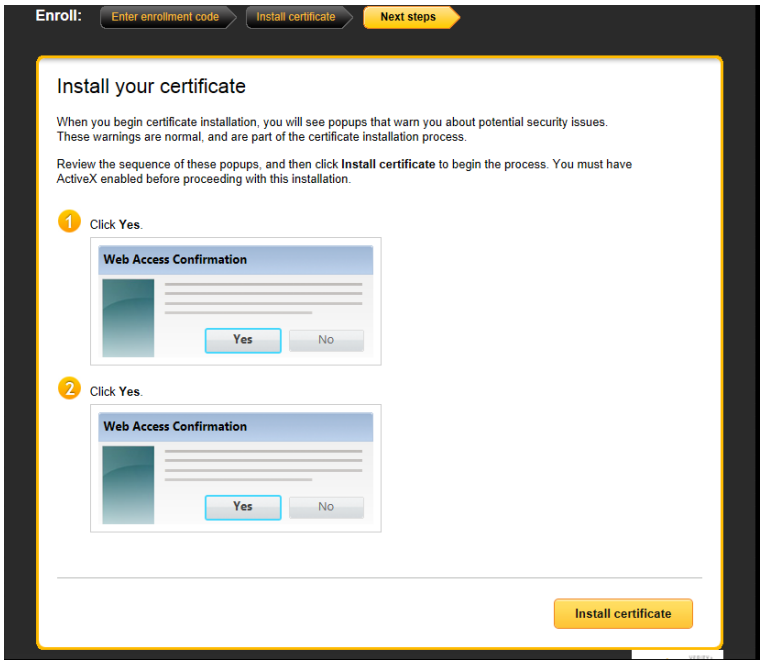
In the "*Add this website:*" field, type ***.symauth.com** then click **Add**, then **Close.**



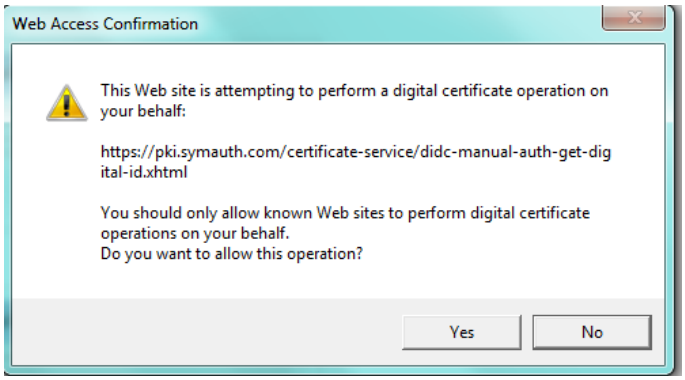
Paste **Enrollment link** into Internet Explorer from the Notepad document
Enter the **Enrollment Code** (also in the notepad document) and click **Continue**.



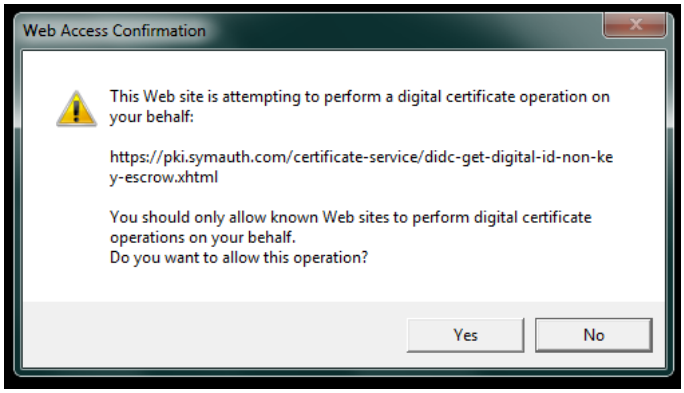
Click **Install Certificate**



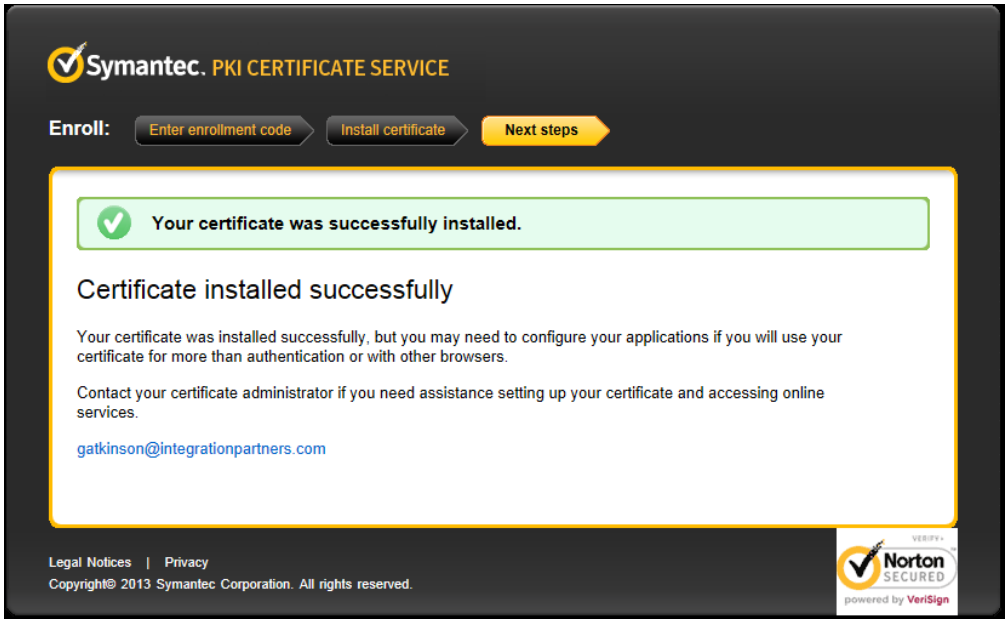
Click **Yes**



Click **Yes**



The certificate should now be installed and you should see this screen

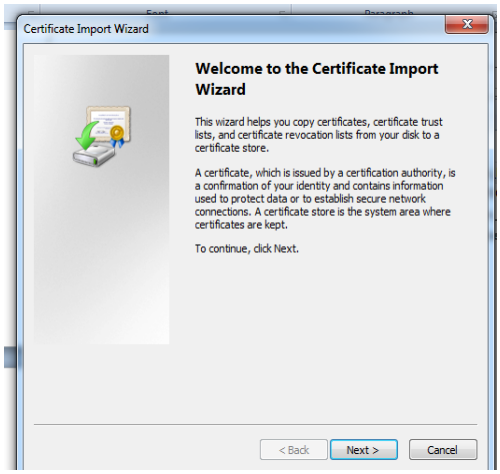


Close the browser.

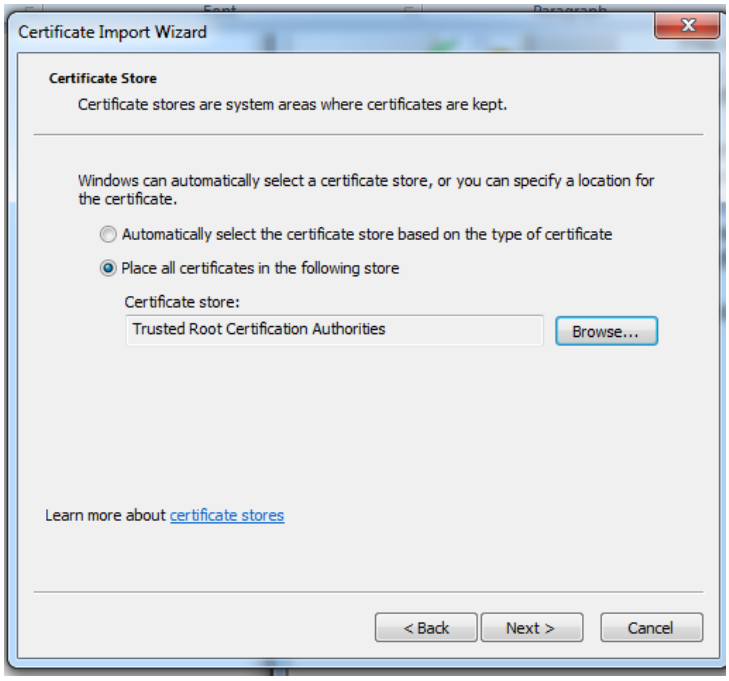
Manual Client Installation

If the automatic process fails, then follow manual steps listed below

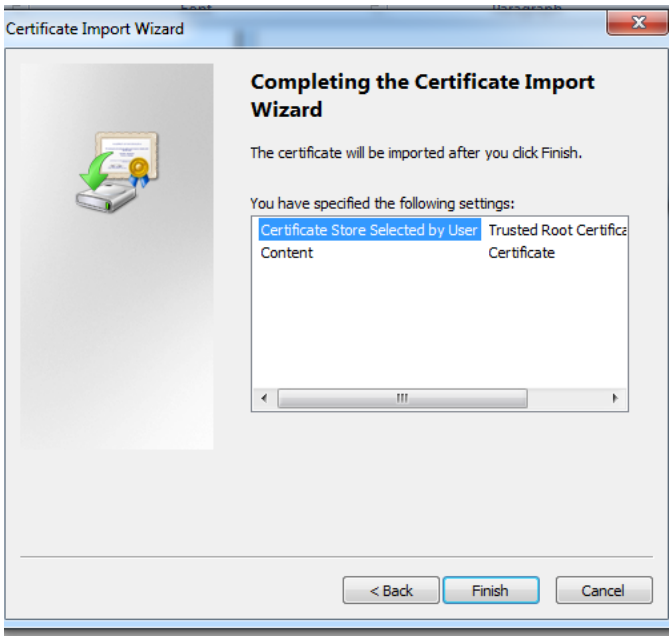
Navigate with Windows Explorer to the C:\otis_v3 folder
Select **ca_public_key.cer** and right click
Click **Install certificate**
Click **next**



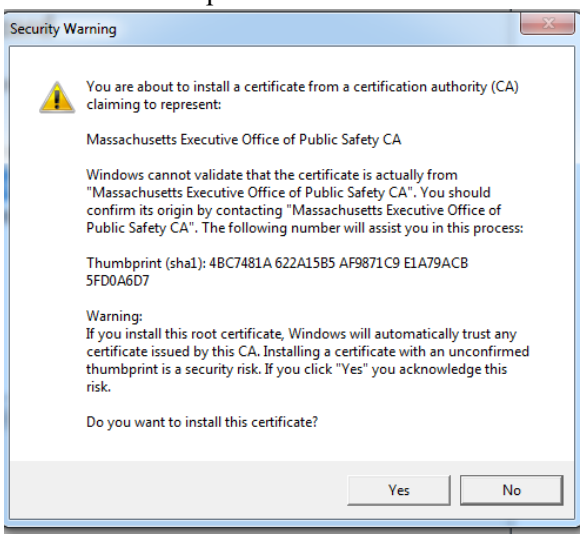
Select the second option, *place all certificates in following store*
Click **Browse** and select Trusted Root Certificate Authorities
Click **next**



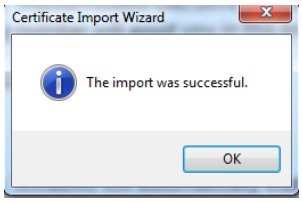
Click **Finish**



Click **Yes** to accept

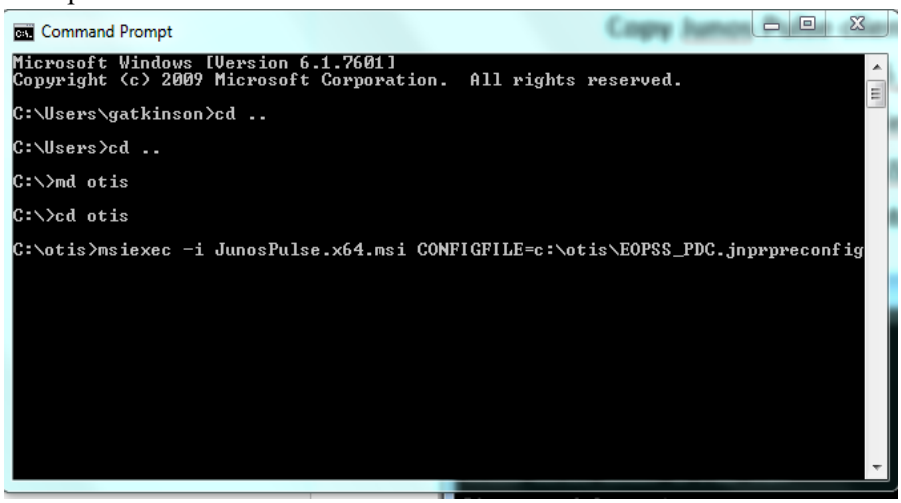


Click **OK**

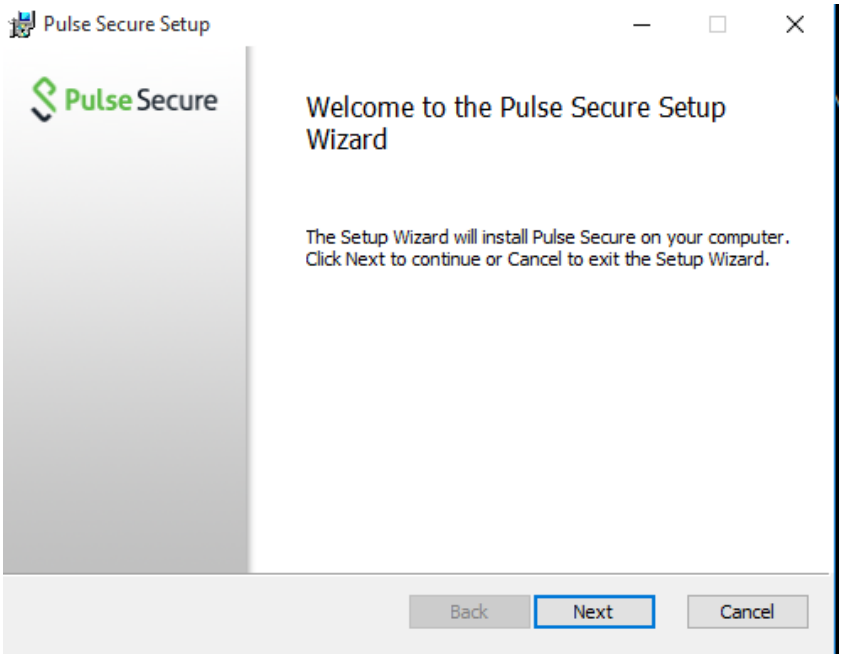


From the DOS prompt
type **c:** then **Enter**
type **CD \otis_v3** then **Enter**
If 64-bit Windows:
Type:
msiexec /i ps-pulse-win-5.2r5.0-b869-64bitinstaller.msi CONFIGFILE=c:\otis_v3\EOPSS_PDC.jnprpreconfig
If 32-bit Windows:
Type:
msiexec /i ps-pulse-win-5.2r5.0-b869-32bitinstaller.msi CONFIGFILE=c:\otis_v3\EOPSS_PDC.jnprpreconfig

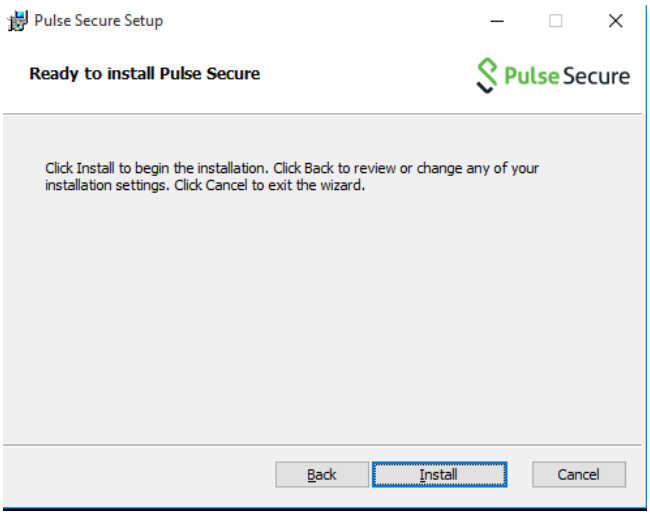
Then press **enter**



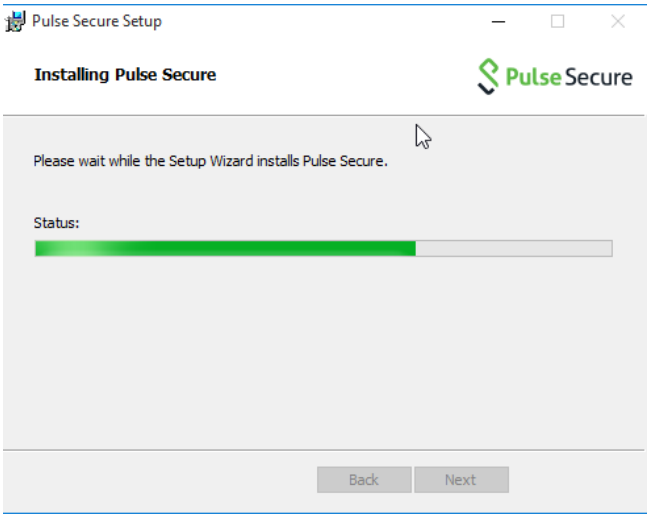
Click **next**



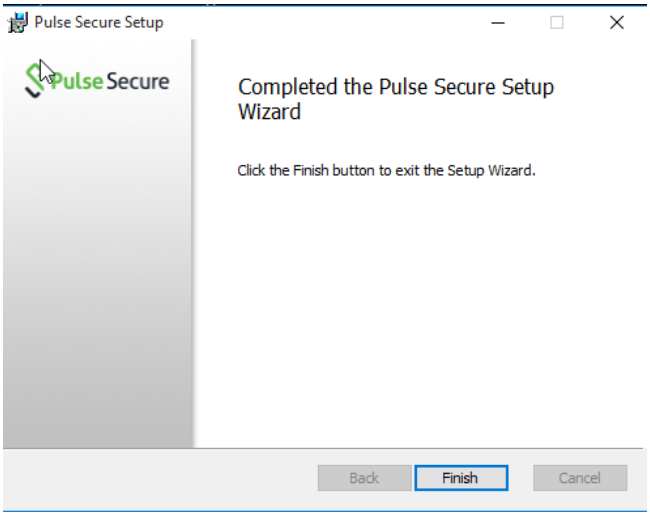
Click **Install**



Installation will begin:



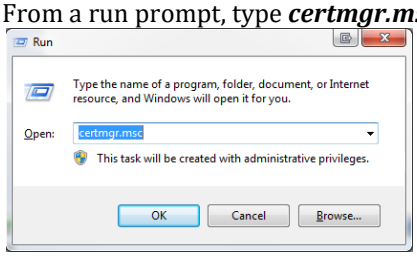
Click **Finish**



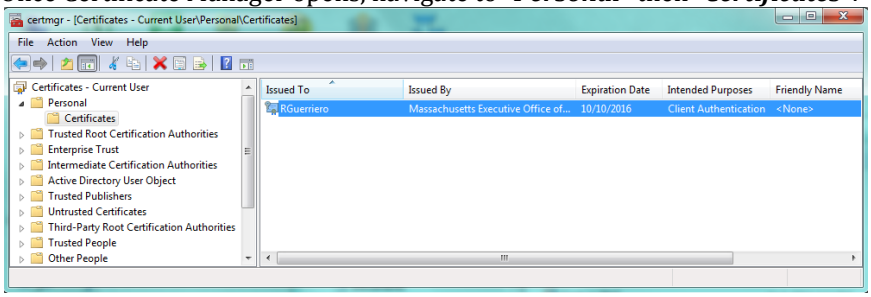
Manual Export of Personal Certificate for Backup purposes or for use on another device

This process can also be used to export a user's certificate from another device in the case where the user has Internet Explorer 11, another non-supported browser or privilege issues.

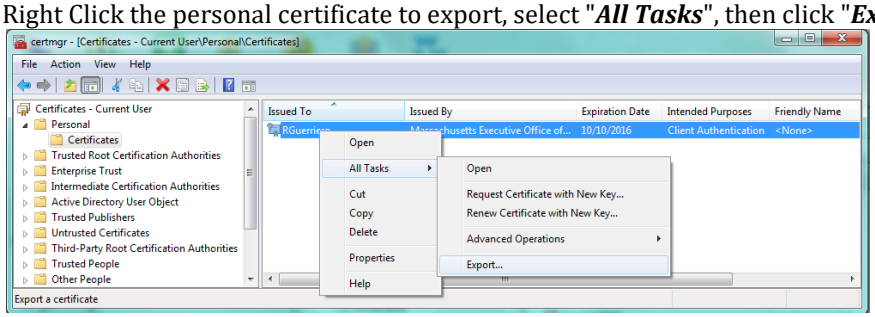
From a run prompt, type ***certmgr.msc*** and click ***OK***:



Once Certificate Manager opens, navigate to "***Personal***" then "***Certificates***":



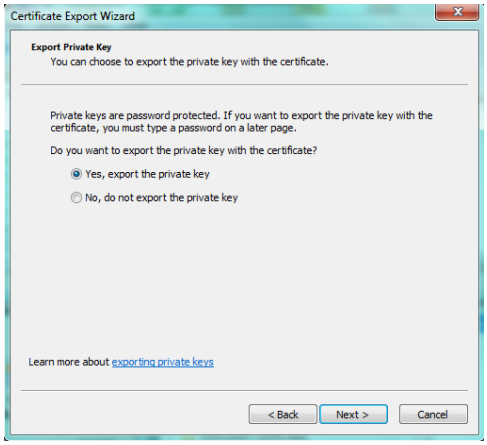
Right Click the personal certificate to export, select "***All Tasks***", then click "***Export…***":



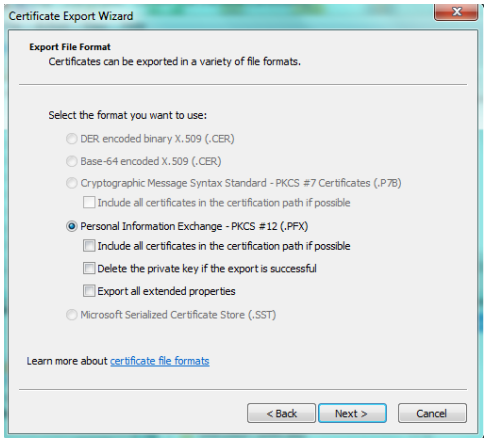
The Certificate Export Wizard will begin, click "***Next***":



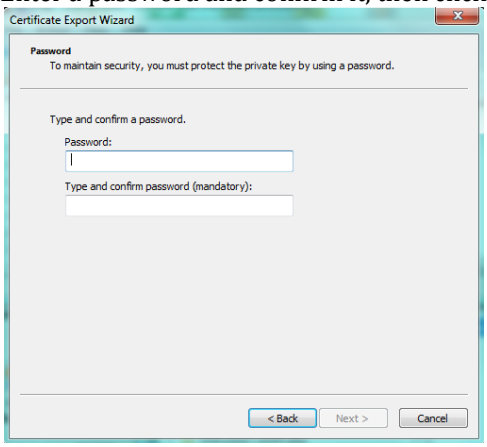
Click the radio button to select "***Yes, export the private key***", then click "***Next***":



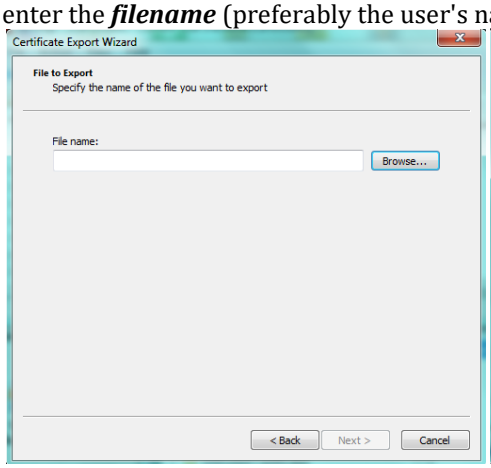
The radio button next to "*Personal Information Exchange*" should be selected and the 3 check boxes blank, click "***Next***":

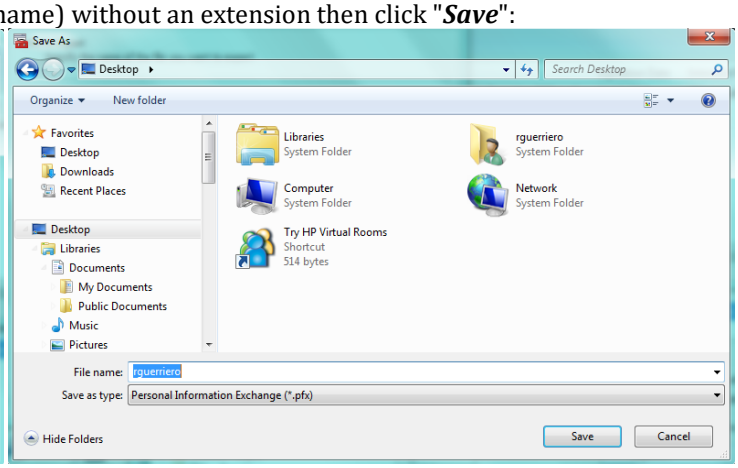


Enter a password and confirm it, then click "***Next***":

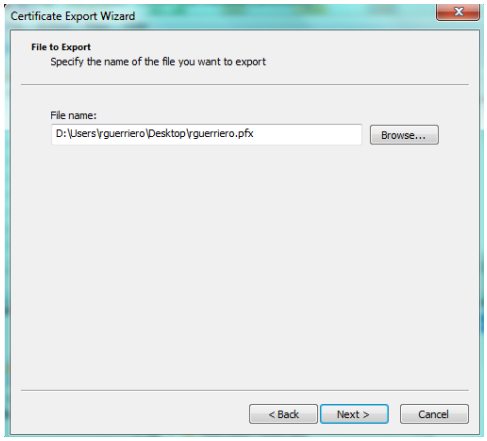


Click "***Browse***", then navigate to a location to store the exported file (in this example, the desktop was used), enter the ***filename*** (preferably the user's name) without an extension then click "***Save***":

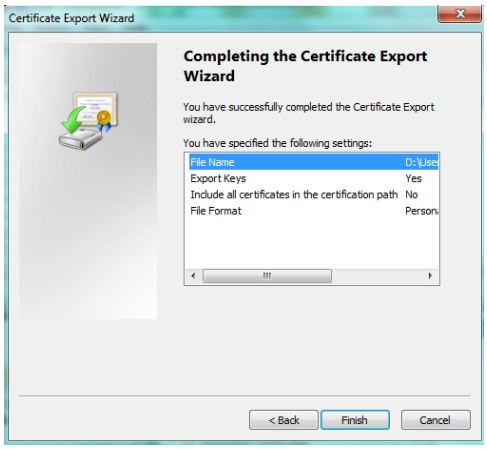




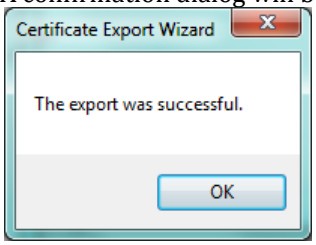
Click "***Next***":



Then click "***Finish***":



A confirmation dialog will be displayed indicating the export was successful, click "***OK***":



Manual Import of Previously Exported Personal Certificate

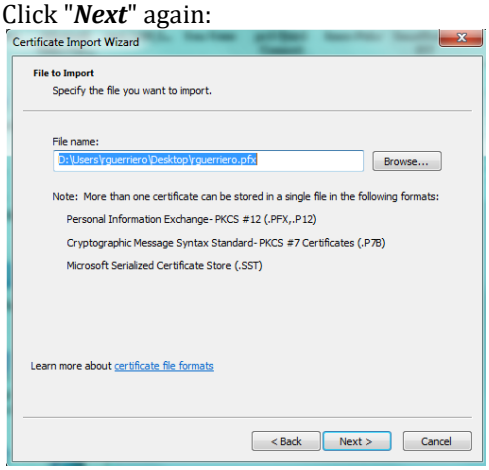
Browse to the location of the exported personal information exchange file (.pfx), then double-click the file:



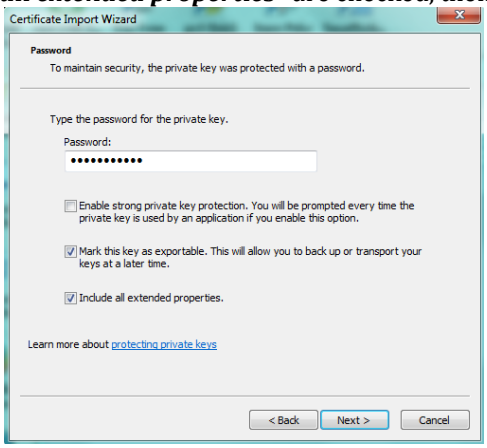
The Certificate Import Wizard will start, click "***Next***":



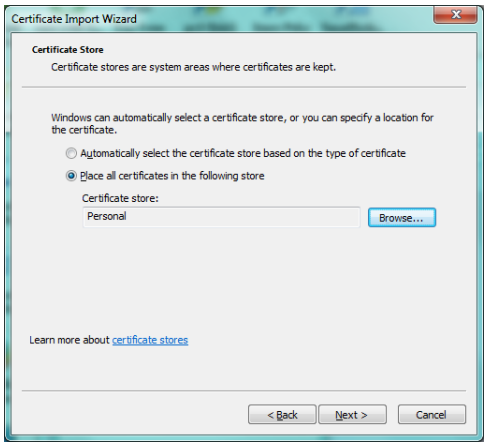
Click "***Next***" again:



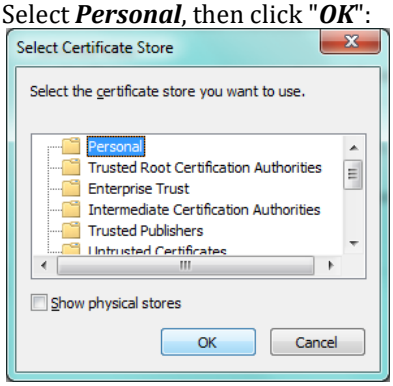
Enter the password the certificate was exported with and ensure "***Mark this key as exportable***" and "***Include all extended properties***" are checked, then click "***Next***":



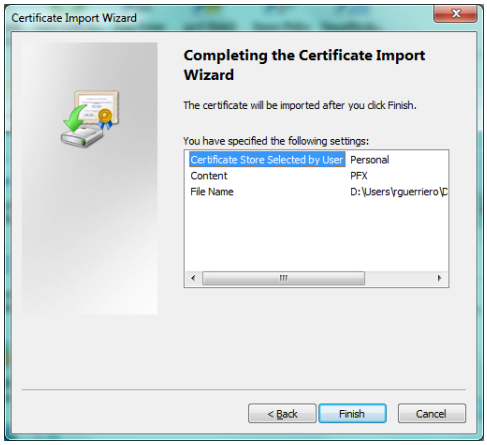
On the next screen, select the radio button next to "***Place all certificates in the following store***" and click the "***Browse...***" button:



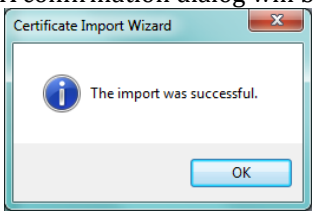
Select ***Personal***, then click "***OK***":



Then click "Finish":



A confirmation dialog will be displayed indicating the import was successful, click "***OK***":



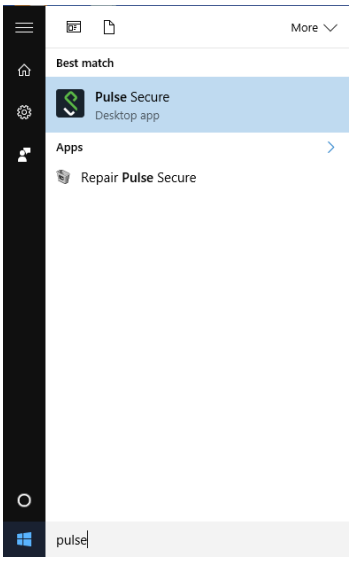
How to use the EOPSS Remote Access Client.

The client should already be installed and configured.

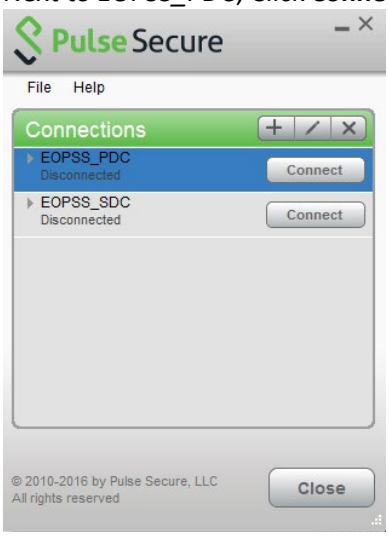
Connecting:

Double Click the Pulse icon that appears in the system tray in the bottom right corner OR Click the Windows icon in the lower left and type Pulse to search for it and click it.





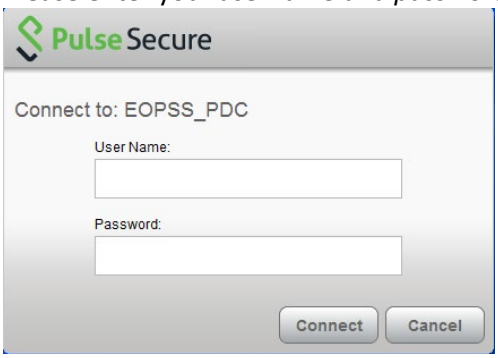
Next to *EOPSS_PDC*, Click ***Connect***



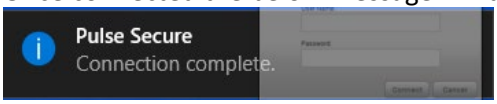
Please note that EOPSS_PDC refers to Primary Data Center which is in Chelsea and EOPSS_SDC refers to Secondary Data Center which is housed in Springfield. ***Either can be used and will provide identical connectivity.***

If you do not get prompted when trying either location, please verify the device has internet connectivity.

Please enter your *username* and *password* and click **Connect**.



Once connected the below message will appear:



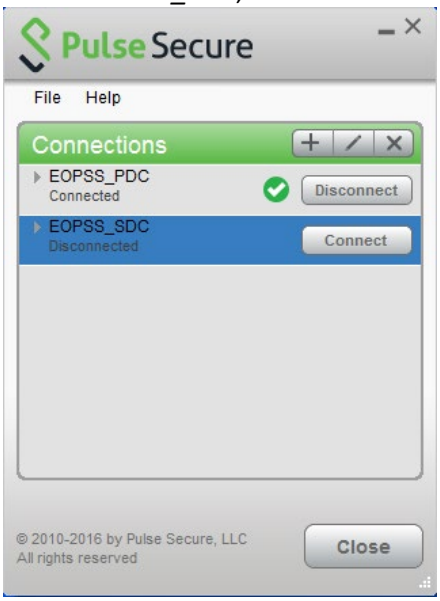
Disconnecting:

Double Click the Pulse icon that appears in the system tray in the bottom right corner OR Click the icon on the desktop

Double Click the Pulse icon that appears in the system tray in the bottom right corner.



Next to *EOPSS_PDC*, Click ***Disconnect***



Access Control Systems

PO Box 7521
Milford, NH 03055

Estimate

Date	Quote #
3/24/2017	QACS17-2053

Name / Address
MA State Police Fusion Ctr Trpr. Brian Egnitz 470 Worcester Road Framingham, MA 01701

Phone #	Fax #	Terms	Project	Rep
603-249-9820	603-249-9818	Net 30		HES

Description	Qty	Cost	Total
ACS-SMT -- Wanco Solar Mast Trailer	[redacted]		421,200.00
500 Watt Solar/3x200Ah AGM Batteries (600 total Ah)			
400 Watt Inverter			
45 Amp Battery Charger			
ACS-WCT-Sierra Wireless GX450 (or equivalent)			72,150.00
ACS-Wanco-Freight (8 units max per shipment)			15,050.00
Systems Installation/Commissioning			0.00
Purchaser to supply: 3M LPR cabling and Controller Equipment Box			
MA FAC64 Compliant Quote			

Accepted Quotes Must Be Signed and Returned With A Purchase Order or Check

Accepted By: _____

Signature: _____

Acceptance Date: _____

This estimate is a "Good Faith" quote of the items proposed. ACS will not be responsible for typos, errors or omissions. Unless otherwise specified, this estimate is valid for acceptance for 30 days from the date issued.

Total **$508,400.00**

Model Policy

	Effective Date **August 2010**	*Number*
Subject **License Plate Readers**		
Reference		*Special Instructions*
Distribution	*Reevaluation Date* **August 2011**	*No. Pages* **3**

I. PURPOSE

The purpose of this policy is to provide officers with guidelines on the proper use of license plate recognition (LPR) systems, also commonly known as license plate reader systems.

II. POLICY

The availability and use of LPR systems have provided many opportunities for the enhancement of productivity, effectiveness, and officer safety. It is the policy of this agency that all members abide by the guidelines set forth herein when using LPR systems.

III. ACRONYMS AND DEFINITIONS

FOUO: For Official Use Only

LPR: License Plate Recognition/License Plate Reader

OCR: Optical Character Recognition

Read: Digital images of license plates and vehicles and associated metadata (e.g., date, time, and geographic coordinates associated with the vehicle image capture) that are captured by the LPR system.

Alert: A visual and/or auditory notice that is triggered when the LPR system receives a potential "hit" on a license plate.

Hit: A read matched to a plate that has previously been registered on an agency's "hot list" of vehicle plates related to stolen vehicles, wanted vehicles, or other factors supporting investigation, or which has been manually registered by a user for further investigation.

Hot list: License plate numbers of stolen cars, vehicles owned by persons of interest, and vehicles associated with AMBER Alerts that are regularly added to "hot lists" circulated among law enforcement agencies. Hot list information can come from a variety of sources, including stolen vehicle information from the National Insurance Crime Bureau and the National Crime Information Center (NCIC), as well as national AMBER Alerts and Department of Homeland Security watch lists. Departments of motor vehicles can provide lists of expired registration tags, and law enforcement agencies can interface their own, locally compiled hot lists to the LPR system. These lists serve an officer safety function as well as an investigatory purpose. In addition to agency supported hot lists, users may also manually add license plate numbers to hot lists in order to be alerted if and when a vehicle license plate of interest is "read" by the LPR system.

Fixed LPR system: LPR cameras that are permanently affixed to a structure, such as a pole, a traffic barrier, or a bridge.

Mobile LPR system: LPR cameras that are affixed, either permanently (hardwired) or temporarily (e.g., magnet-mounted), to a law enforcement vehicle for mobile deployment.

Portable LPR system: LPR cameras that are transportable and can be moved and deployed in a variety of venues as needed, such as a traffic barrel or speed radar sign.

IV. PROCEDURES

A. General

1. The use of LPR systems is restricted to public safety–related missions of this agency.
2. LPR systems and associated equipment and databases are authorized for official public safety purposes. Misuse of this equipment and associated databases, or data, may be subject to sanctions and/or disciplinary actions.
3. LPR systems and LPR data and associated

media are the property of this agency and intended for use in conducting official business with limited exceptions noted elsewhere in this policy.

B. Administration
   1. The agency shall designate an employee(s) with administrative oversight for LPR system deployment and operations who is (are) responsible for the following:
      a. Establishing protocols for access, collection, storage, and retention of LPR data and associated media files
      b. Establishing protocols to preserve and document LPR reads and "alerts" or "hits" that are acted on in the field or associated with investigations or prosecutions
      c. Establishing protocols to establish and ensure the security and integrity of data captured, stored, and/or retained by the LPR system
      d. Ensuring the proper selection of the personnel approved to operate the LPR system and maintaining an adequate number of trainees;
      e. Maintaining records identifying approved LPR deployments and documenting their results, including appropriate documentation of significant incidents and arrests that are related to LPR usage
      f. Authorizing any requests for LPR systems use or data access according to the policies and guidelines of this agency
   2. Designated, trained personnel shall check equipment on a regular basis to ensure functionality and camera alignment. Any equipment that falls outside expected functionality shall be removed from service until deficiencies have been corrected.
   3. LPR systems repairs, hardware or software, shall be made by agency authorized sources.

C. License Plate Reader System Usage
   1. LPR operation and access to LPR collected data shall be for official agency purposes only.
   2. Only officers who have been properly trained in the use and operational protocols of the LPR systems shall be permitted to use it.
   3. At the start of each shift users must ensure that the LPR system has been updated with the most current hot lists available.
   4. LPR Alerts/Hits: Prior to initiation of the stop:
      a. Visually verify that the vehicle plate number matches the plate number run by the LPR system, including both alphanumeric characters of the license plate and the state of issuance.
      b. Verify the current status of the plate through dispatch or MDT query when circumstances allow.
   5. In each case in which an alert or a hit is triggered, the user should record the disposition of the alert and the hit into the LPR system
   6. Hot lists may be updated manually if the user enters a specific plate into the LPR system and wants to be alerted when that plate is located. Whenever a plate is manually entered into the LPR system, the officer should document the reason.
   7. Special Details: LPR use during nontraditional deployments (e.g., special operations or during a criminal investigation) must be approved by the administrator.
   8. Searches of historical data within the LPR system should be done in accordance with established departmental policies and procedures.

D. LPR Data Sharing and Dissemination
   LPR data should be considered FOUO and can be shared for legitimate law enforcement purposes:
   1. When LPR data are disseminated outside the agency, it should be documented in a secondary dissemination log.
   2. Information sharing among agencies should be dictated in accordance with MOUs (memoranda of understanding) or established departmental policies.

E. Retention
   Please refer to the *License Plate Reader Concepts and Issues Paper* for a discussion on retention.

Acknowledgment

This *Model Policy* was developed by the International Association of Chiefs of Police (IACP) Law Enforcement Information Management (LEIM) Section, in cooperation with the IACP National Law Enforcement Policy Center. Additional support was provided by the LPR Model Policy Working Group, to whom we are deeply appreciative for sharing their agency policies and expertise.

Every effort has been made by the IACP National Law Enforcement Policy Center staff and advisory board to ensure that this model policy incorporates the most current information and contemporary professional judgment on this issue. However, law enforcement administrators should be cautioned that no "model" policy can meet all the needs of any given law enforcement agency. Each law enforcement agency operates in a unique environment of federal court rulings, state laws, local ordinances, regulations, judicial and administrative decisions and collective bargaining agreements that must be considered. In addition, the formulation of specific agency policies must take into account local political and community perspectives and customs, prerogatives and demands; often divergent law enforcement strategies and philosophies; and the impact of varied agency resource capabilities among other factors.

This project was supported by Grant No. 2006-DG-BX-K004 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. The Assistant Attorney General, Office of Justice Programs, coordinates the activities of the following program offices and bureaus: the Bureau of Justice Assistance, the Bureau of Justice Statistics, National Institute of Justice, Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice or the IACP.

© Copyright 2010. International Association of Chiefs of Police, Alexandria, Virginia U.S.A. All rights reserved under both international and Pan-American copyright conventions. No reproduction of any part of this material may be made without prior written consent of the copyright holder.

MMARS DOCUMENT ID: **ISAEPSJG16HEROPOL18A**

411

COMMONWEALTH OF MASSACHUSETTS
INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM

This Form is issued and published by the Office of the Comptroller (CTR) pursuant to 815 CMR 6.00 for use by all Commonwealth Departments. Departments may add non-conflicting additional terms, but changes to the official printed language of this Form shall be void.

BUDGET FISCAL YEAR: 2018	RFR REFERENCE NUMBER ENTER RFR NUMBER: OR __X__ N/A.
MMARS ALPHA *BUYER/PARENT* DEPARTMENT CODE: EPS	MMARS ALPHA *SELLER/CHILD* DEPARTMENT CODE: POL
BUSINESS MAILING ADDRESS: 10 PARK PLAZA, SUITE 3720 BOSTON, MA 02116	BUSINESS MAILING ADDRESS: MASSACHUSETTS DEPARTMENT OF STATE POLICE 470 WORCESTER ROAD FRAMINGHAM, MA 01702
ISA MANAGER: PAUL GARRITY	ISA MANAGER: DEBORAH J. BRODERICK
PHONE: **617-725-3322** FAX: 617-725-0260	PHONE: **508-820-2300** FAX: 508-820-2359
E-MAIL ADDRESS: PAUL.GARRITY@STATE.MA.US	E-MAIL ADDRESS: DEBORAH.BRODERICK@MASSMAIL.STATE.MA.US

Purpose of ISA: (Check one option only and complete applicable information) (Attachment A required for New ISAs and all ISA Amendments.)

__X__ New ISA. Current Maximum Obligation for total duration of ISA $ 97,946.80 (Use "N/A" for Non-Financial ISA.) (Complete Attachment B)

____ Amendment to Existing ISA. What is being amended? (Attachment C required for all Federal and Bond Account Amendments)

- ____ Amend Budget/Accounts. Change Maximum Obligation from: $_____ to New Maximum Obligation $_____ (Attachment B)
- ____ Amend Budget/Accounts. No Change in Maximum Obligation (Attachment B)
- ____ Amend Dates of Performance. New Dates of Service: Start Date:_____End Date:_____(Subject to execution dates below.)
- ____ Amend Scope of Services/Performance

BRIEF DESCRIPTION OF PERFORMANCE GOALS TO BE ACCOMPLISHED BY ISA, OR IF AMENDMENT, IDENTIFY WHAT IS BEING AMENDED: TO FUND THE HEROIN AND OPIOID PROGRAM

WILL SELLER/CHILD DEPARTMENT STATE EMPLOYEES (AA OBJECT CLASS) BE FULLY OR PARTIALLY FUNDED UNDER THIS ISA? **__X__ No ____ Yes.** If Yes, Seller/Child certifies that the ISA is not being used as an alternative funding mechanism for state employees, that the identified personnel in Attachment A are necessary for completion of the ISA due to particular expertise or other factors that can not be obtained through the use of contractors, and that if federal funds are being used, funds shall not be used to supplement the regular salary or compensation of any officer or employee of the Commonwealth for services performed during their regular working hours. M.G.L. c. 29, § 6B.

ACCOUNT INFORMATION. Complete for all new ISAs and Amendments (even if account information is not changing) Check one option, indicate "add", "delete" or "no change" and enter account, fund, major program code and program code.

__x__ BGCN – non-subsidiarized (federal, capital, trust). Attachment C required for any new ISA or ISA Amendment involving federal funds.
____ BGCS – subsidiarized (budgetary)
____ Other (CT, RPO as authorized by CTR): _____.
____ Non-Financial ISA (no funds are transferred from Buyer/Parent to Seller/Child), however, resources are committed to ISA.
____ Amendment with no Accounting Changes to Budget/Accounts or to Attachments B or C. (Indicate no change below and complete account information.)

__X__ ADD __ DELETE __ NO CHANGE	Account:80004611	Fund: 0100	Major Program Code: BJAG	Program Code: FJG1HEOP16
__ ADD __ DELETE __ NO CHANGE	Account:	Fund:	Major Program Code:	Program Code:
__ ADD __ DELETE __ NO CHANGE	Account:	Fund:	Major Program Code:	Program Code:
__ ADD __ DELETE __ NO CHANGE	Account:	Fund:	Major Program Code:	Program Code:

ISA ANTICIPATED START DATE: **12/01/2017** provided that the Seller/Child certifies that it will not incur any obligations related to this ISA prior to the date that this ISA is executed, NOR prior to the date that sufficient funding for the obligations for this ISA is available in the Seller/Child account for expenditure.

TERMINATION DATE OF THIS ISA: This ISA shall terminate on **11/30/2018** unless terminated or properly amended in writing by the parties prior to this date.

BUYER/PARENT AND SELLER/CHILD DEPARTMENT CERTIFICATIONS. IN WITNESS WHEROF, by executing this ISA below, the Buyer/Parent and Seller/Child certify, under the pains and penalties of perjury, that Buyer/Parent and Seller/Child understand and agree that any Buyer/Parent or Seller/Child officer or employee who knowingly violates, authorizes or directs another officer or employee to violate any provision of state finance law relating to the incurring of liability or expenditure of public funds, includng this ISA, may be considered to be in violation of M.G.L. c. 29, § 66, and therefore the Buyer/Parent and the Seller/Child agree to ensure that this ISA complies with, and that all staff or contractors involved with ISA performance are provided with sufficient training and oversight to ensure compliance with 815 CMR 6.00, CTR applicable policies and the ISA Terms and Conditions which are incorporated by reference into this ISA, in addition to the performance requirements identified in Attachnent A of this ISA, and that all terms governing performance of this ISA are attached to this ISA or incorporated by reference herein, and the Buyer/Parent and Seller/Child agree to maintain the necessary level of communication (including immediate notification of any amendments to accounting information, program codes or performance needs), coordination, access to reports and other ISA information, and cooperation to ensure the timely execution and successful completion of the ISA, amendments, and state finance law compliance; and that the Buyer/Parent certifies it will ensure that sufficient funds are timely made available in the Seller/Child account(s), with the proper accounting codes, prior to the Seller/Child's need to begin initial or amended performance; and that the Seller/Child will not allow initial or amended performance to begin until the ISA is executed AND the ISA Seller/Child account is sufficiently funded to support encumbrances and payments for performance (including payroll), and the Seller/Child will make encumbrances and payments (including payroll) only from the authorized ISA Seller/Child account(s) and shall not be entitled to transfer charges made from any other account not approved in writing by CTR in advance of expenditures by the Seller/Child.

20BUYER/PARENT DEPARTMENT'S AUTHORIZED SIGNATURE: **DATE:** (Date must be handwritten by signatory at time of signature)	**SELLER/CHILD DEPARTMENT'S AUTHORIZED SIGNATURE:** **DATE:** (Date must be handwritten by signatory at time of signature)
PRINT NAME: ANGELA F. F. DAVIS	PRINT NAME: MICHELLE SMALL
PRINT TITLE: EXECUTIVE DIRECTOR	PRINT TITLE: CHIEF ADMINISTRATIVE OFFICER

ISAEPSJG16HEROPOL18A

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM

TERMS AND CONDITIONS

The following terms and conditions are incorporated by reference into any ISA.

Role of the Office of the Comptroller. All ISA fiscal transactions shall be made through the state accounting system as prescribed by the Office of the Comptroller (CTR). CTR will interpret 815 CMR 6.00 and applicable policies and take any fiscal or other actions necessary to ensure ISA compliance with state finance law, including but not limited to correcting accounting transactions, resolving ISA disputes and identifying corrective action by the Buyer/Parent or Seller/Child Departments.

Seller/Child Department Certifications. By executing an ISA the Seller/Child certifies that it is statutorily authorized to provide the type of performance sought by the Buyer/Parent, and shall at all times remain qualified to perform the ISA, that performance shall be timely and meet or exceed ISA standards, that the Seller/Child will not allow initial or amended performance to begin, may not authorize personnel or contractors to work, nor incur any obligation to be funded under an ISA prior to the execution of an ISA AND the availability of ISA funding in the Seller/Child account to support encumbrances and payments for performance. The Seller/Child will make encumbrances and payments (incuding payroll) only from the authorized ISA Seller/Child account(s) and shall not be entitled to transfer charges made from any other account not approved in writing in advance by CTR. The Seller/Child must immediately notify CTR whenever a delay in funding is anticipated for which performance is expected. The Seller/Child is authorized to use ISA funding only for the actual costs of ISA performance and may not use ISA funds to supplement non-ISA related personnel or expenditures.

Buyer/Parent Department Certifications. Signature by the Buyer/Parent certifies that it is statutorily authorized or required to procure the type of performance required under this ISA, that the Buyer/Parent certifies it will ensure that sufficient funds are timely made available in the Seller/Child Seller/Child account(s), with the proper accounting codes, prior to the Seller/Child's need to begin intial or amended performance; that the Buyer/Parent will monitor and reconcile ISA performance in compliance with state appropriation language or federal grant requirements, communicate all fiscal information necessary for the set up of the Seller/Child account(s) including budget information, and if the ISA is funded with federal funds provide accurate accounting information in Attachment C, and immediately notify the Seller/Child of any changes in Attachment C (such as program codes) to ensure the ISA and Seller/Child account can be timely updated to avoid lapses in funding or the inability of the Seller/Child to make timely payroll and other expenditures from the Seller/Child account.

Chief Fiscal Officer. The Chief Fiscal Officer (CFO) for the Buyer/Parent and Seller/Child will be responsible for the fiscal management of ISAs within their Departments in accordance with these ISA Terms and Conditions, 815 CMR 6.00 and policies and procedures published by CTR.

ISA Manager. Both the Buyer/Parent and Seller/Childs are responsible for ensuring that the ISA Manager listed on the ISA, or ISA Amendment, is current and that the ISA Manager is an authorized signatory for the Department supported by the appropriate Security Profile. If the listed ISA Manager changes, the CFO shall be the ISA Manager until a replacement is identified in the same manner as other Written Notice.

Record-keeping and Retention, Inspection of Records. The Buyer/Parent and Seller/Child shall maintain all ISA records in such detail as necessary to support claims for payment, including reimbursement or federal financial participation (FFP), for at least seven (7) years from the last payment under an ISA Seller/Child account, or such longer period as is necessary for the resolution of any litigation, claim, negotiation, audit or other inquiry involving an ISA. In addition to any specific progress, programmatic or expenditure reports specified in Attachment A, the Seller/Child is required to provide the Buyer/Parent (and to CTR, the State Auditor and the House and Senate Ways and Means Committees upon request) with full cooperation and access to all ISA information.

Payments and Compensation. The Seller/Child may accept compensation only for performance delivered and accepted by the Buyer/Parent in accordance with the specific terms and conditions of the ISA. All ISA payments are subject to appropriation pursuant to M.G.L. C. 29, or the availability of sufficient non-appropriated funds for the purposes of an ISA. Overpayments or disallowed expenditures shall be reimbursed by the Seller/Child or may be offset from future ISA payments in accordance with state finance law and instructions from CTR.

ISA Termination or Suspension. An ISA shall terminate on the date specified, unless this date is properly amended prior to this date, or unless terminated or suspended under this Section upon prior written notice to the Seller/Child. The Buyer/Parent may terminate an ISA without cause and without penalty with at least thirty days prior written notice, or may terminate or suspend an ISA with reasonable notice if the Seller/Child breaches any material term or condition or fails to perform or fulfill any material obligation required by an ISA, or in the event of an elimination of an appropriation or availability of sufficient funds for the purposes of an ISA, or in the event of an unforeseen public emergency mandating immediate Buyer/Parent action. Upon immediate notification to the other party, neither the Buyer/Parent nor the Seller/Child shall be deemed to be in breach for failure or delay in performance due to Acts of God or other causes factually beyond their control and without their fault or negligence. Contractor failure to perform or price increases due to market fluctuations or product availability will not be deemed factually beyond the Seller/Child's control.

Written Notice. Any notice shall be deemed delivered and received when submitted in writing in person or when delivered by any other appropriate method evidencing actual receipt by the Buyer/Parent or the Seller/Child. Unless otherwise specified in the ISA, legal notice sent or received by the Buyer/Parent's ISA Manager or the CFO (with confirmation of actual receipt) through the listed fax number(s) or E-Mail address for the ISA Manager will satisfy written notice under the ISA. Any written notice of termination or suspension delivered to the Seller/Child shall state the effective date and period of the notice, the reasons for the termination or suspension, if applicable, any alleged breach or failure to perform, a reasonable period to cure any alleged breach or failure to perform, if applicable, and any instructions or restrictions concerning allowable activities, costs or expenditures by the Seller/Child during the notice period.

Confidentiality. The Seller/Child shall comply with M.G.L. C. 66A if the Seller/Child becomes a "holder" of "personal data". The Seller/Child shall also protect the physical security and restrict any access to personal or other Buyer/Parent data in the Seller/Child's possession, or used by the Seller/Child in the performance of an ISA, which shall include, but is not limited to the Buyer/Parent's public records, documents, files, software, equipment or systems. If the Seller/Child is provided access with any other data or information that triggers confidentiality requirements under FIPA, HIPPA or other federal or state laws, the Seller/Child shall be responsible for protection of this data as instructed by the Buyer/Parent.

Assignment. The Seller/Child may not assign, delegate or transfer in whole or in part any ISA, or any liability, responsibility, obligation, duty or interest under an ISA, to another Department or an outside contractor. Assumption of an ISA by a successor Department due to a legislative change in the Seller/Child or Buyer/Parent's department status shall be accomplished through the execution of a new ISA.

Subcontracting By Seller/Child. Since it is presumed that contracting through the Seller/Child is more cost effective and a better value than the Buyer/Parent directly contracting with an outside contractor(s), any subcontract entered into by the Seller/Child for the purposes of fulfilling the obligations under an ISA must be approved by the Buyer/Parent in advance of the ISA and justified as part of the ISA Attachment A. The Seller/Child is responsible for full state finance law and procurement compliance for all subcontracts, and shall supply a copy of any subcontract to the Buyer/Parent upon request.

Affirmative Action, Non-Discrimination in Hiring and Employment. In performing this ISA, the Seller/Child shall comply with all federal and state laws, rules, regulations and applicable internal state policies and agreements promoting fair employment practices or prohibiting employment discrimination and unfair labor practices and shall not discriminate in the hiring of any applicant for employment nor shall any qualified employee be demoted, discharged or otherwise subject to discrimination in the tenure, position, promotional opportunities, wages, benefits or terms and conditions of their employment because of race, color, national origin, ancestry, age, sex, religion, disability, handicap, sexual orientation or for exercising any rights afforded by law. The Seller/Child commits to, when possible, to purchasing supplies and services from certified minority or women-owned businesses, small businesses or businesses owned by socially or economically disadvantaged persons or persons with disabilities in accordance with the Commonwealth's Affirmative Market Program.

Waivers. Forbearance, indulgence or acceptance by the Seller/Child or Buyer/Parent of any breach or default in any form shall not be construed as a waiver and shall not limit enforcement remedies or allow a waiver of any subsequent default or breach.

Risk of Loss. The Seller/Child shall bear the risk of loss for any materials, deliverables, personal or other data that is in the possession of the Seller/Child or used by the Seller/Child in the performance of an ISA until is accepted by the Buyer/Parent.

Disputes. The Buyer/Parent and Seller/Child agree to take all necessary actions to resolve any dispute arising under the ISA within 30 calendar days including department head and secretariat involvement, but in no event shall a dispute remain unresolved beyond May 30th in any fiscal year, nor may the Buyer/Parent or Seller/Child allow a dispute to create a state finance law or other violation of ISA terms (such as a delay in funding, failure to timely communicate funding or program code changes, or failure to timely process ISA paperwork). Seller/Child and Buyer/Parent must immediately notify CTR to assist in resolution of the dispute and shall implement any actions required by CTR to resolve the dispute, which shall be considered final.

Interpretation, Severability, Conflicts with Law, Integration. Any amendment or attachment to any ISA that contains conflicting language or has the affect of deleting, replacing or modifying any printed language of the ISA shall be interpreted as superseded by the ISA Form as published. If any ISA provision is superseded by state or federal law or regulation, in whole or in part, then both parties shall be relieved of all obligations under that provision to the extent necessary to comply with the superseding law, provided however, that the remaining provisions of the ISA, or portions thereof, shall be enforced to the fullest extent permitted by law. The terms of this ISA shall survive its termination for the purpose of resolving any claim, dispute or other action, or for effectuating any negotiated representations and warranties.

ISAEPSJG16HEROPOL18A

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM

TERMS AND CONDITIONS

ATTACHMENT A – TERMS OF PERFORMANCE AND JUSTIFICATIONS:

This Attachment Form must be used. Insert (type or copy and paste) all relevant information using as many pages as necessary. Attach any additional supporting documentation as appropriate. If Amending the ISA, completion of Sections 1, 2 and 3 identifying what is being amended and the reasons for the amendments is required. For sections 4-9 enter only the amended language in the sections being amended.

1. [REQUIRED] Purpose and other performance goals of ISA, or as amended:

The Massachusetts State Police (MSP) created a fifth division, called the Division of Homeland Security and Preparedness (referred to herein as DHS) and tasked it with spearheading the state's opioid interdiction efforts to combat the opioid epidemic. This project will support this mission with the purchase of Automated License Plate Readers (ALPR), which can be used for suspect specific opioid distribution and trafficking investigations. Additional equipment will be purchased to exploit the telephonic communications made by opioid distributors and traffickers.

2. [REQUIRED] Identify in detail, the responsibilities of the parties, the scope of services and terms of performance under the ISA, or as amended:

- A Uniform Branch Captain will serve as the project manager for grant reporting requirements and will work with MSP Finance Section to ensure that all equipment is purchased in accordance with applicable state procurement laws.
- MSP Fiscal Section will oversee the financial reporting requirements and will ensure the timely completion and submission of all fiscal documents.
- To combat the opioid epidemic, the Massachusetts State Police created a fifth division, called the Division of Homeland Security and Preparedness (referred to herein as DHS) and tasked it with spearheading the state's opioid interdiction efforts. This project will support this mission with the purchase of Automated License Plate Readers (ALPR), which can be used for suspect specific opioid distribution and trafficking investigations. Additional equipment will be purchased to exploit the telephonic communications made by opioid distributors and traffickers.

3. [REQUIRED] Identify schedule of performance or completion dates or other benchmarks for performance, or as amended:

All purchasing will be completed prior to the end date of the ISA 11/30/2018**.**

4. [REQUIRED] Justification that use of ISA is best value vs. contract with outside vendor:

The MSP has designated the DHSP and the SPEAR Center as the lead in this law enforcement and public safety project. An outside vendor is not appropriate for this project.

5. Will Seller/Child department state employees (AA Object Class) be fully or partially funded under this ISA? __X__ No
Yes. If Yes, justify necessity to use state employees for the ISA vs. use of contractors (contract employees or outside vendors).

6. Subcontractors. Since it is presumed that contracting through the Seller/Child is more cost effective and a better value than the Buyer/Parent directly contracting with an outside contractor(s), any subcontract entered into by the Seller/Child for the purposes of fulfilling the obligations under an ISA must be approved by the Buyer/Parent in advance of the ISA and justified as part of the ISA Attachment A, as follows: (enter "N/A" if subcontractors will not be funded with ISA funds)

N/A

7. Identify any equipment that will be leased or purchased by the Seller/Child using ISA funds: (The Buyer/Parent shall determine ownership of equipment purchased by the Seller/Child with ISA funds. Enter "N/A" if equipment not included in ISA.)

This MSP will purchase commodities that will assist in combating the opioid epidemic. The purchase of equipment includes Automated License Plate Readers (ALPR), which can be used for suspect specific opioid distribution and trafficking investigations. Additional equipment will be purchased to exploit the telephonic communications made by opioid distributors and traffickers such as ALPR cameras, accessories for ALPR cameras, IT equipment and software to be used with the ALPR. All equipment will be added to the inventory of the MSP.

If equipment will be purchased with federal funds, please complete Attachment B to reflect the obligation for this purchase. Additionally, the seller must adhere to the federal guidelines for equipment purchased with federal grant funds included in this section.

Federal Guidelines on Equipment

The following are the guidelines on equipment found in the Federal Uniform Administrative Requirements for Grants document. As the name implies, these guidelines apply to all federal grant programs. While previously referred to as Federal OMB Circular A-102, it is now codified by each of the OGR federal granting agencies within various sections of the Code of Federal Regulations. The sections on equipment are as follows:

(a) *Title.* Subject to the obligations and conditions set forth in this section, title to equipment acquired under a grant or subgrant will vest upon acquisition in the grantee or subgrantee respectively.

(b) *States.* A State will use, manage, and dispose of equipment acquired under a grant by the State in accordance with State laws and procedures. Other grantees and subgrantees will follow paragraphs (c) through (e) of this section.

(Massachusetts State Government procedures can be found in the next section)

(c) *Use.* (1) Equipment shall be used by the grantee or subgrantee in the program or project for which it was acquired as long as needed, whether or not the project or program continues to be supported by Federal funds. When no longer needed for the original program or project, the equipment may be used in other activities currently or previously supported by a Federal agency.

(2) The grantee or subgrantee shall also make equipment available for use on other projects or programs currently or previously supported by the Federal Government, providing such use will not interfere with the work on the projects or program for which it was originally acquired. First preference for other use shall be given to other programs or projects supported by the awarding agency. User fees should be considered if appropriate.

(3) Notwithstanding the encouragement in §18.25(a) to earn program income, the grantee or subgrantee must not use equipment acquired with grant funds to provide services for a fee to compete unfairly with private companies that provide equivalent services, unless specifically permitted or contemplated by Federal statute.

(4) When acquiring replacement equipment, the grantee or subgrantee may use the equipment to be replaced as a trade-in or sell the property and use the proceeds to offset the cost of the replacement property, subject to the approval of the awarding agency.

(d) *Management requirements.* Procedures for managing equipment (including replacement equipment), whether acquired in whole or in part with grant funds, until disposition takes place will, as a minimum, meet the following requirements:

(1) Property records must be maintained that include a description of the property, a serial number or other identification number, the source of property, who holds title, the acquisition date, and cost of the property, percentage of Federal participation in the cost of the property, the location, use and condition of the property, and any ultimate disposition data including the date of disposal and sale price of the property.

(2) A physical inventory of the property must be taken and the results reconciled with the property records at least once every two years.

(3) A control system must be developed to ensure adequate safeguards to prevent loss, damage, or theft of the property. Any loss, damage, or theft shall be investigated.

(4) Adequate maintenance procedures must be developed to keep the property in good condition.

(5) If the grantee or subgrantee is authorized or required to sell the property, proper sales procedures must be established to ensure the highest possible return.

(e) *Disposition.* When original or replacement equipment acquired under a grant or subgrant is no longer needed for the original project or program or for other activities currently or previously supported by a Federal agency, disposition of the equipment will be made as follows:

(1) Items of equipment with a current per-unit fair market value of less than $5,000 may be retained, sold or otherwise disposed of with no further obligation to the awarding agency.

(2) Items of equipment with a current per unit fair market value in excess of $5,000 may be retained or sold and the awarding agency shall have a right to an amount calculated by multiplying the current market value or proceeds from sale by the awarding agency's share of the equipment.

(3) In cases where a grantee or subgrantee fails to take appropriate disposition actions, the awarding agency may direct the grantee or subgrantee to take excess and disposition actions.

(f) *Federal equipment.* In the event a grantee or subgrantee is provided federally-owned equipment:

(1) Title will remain vested in the Federal Government.

(2) Grantees or subgrantees will manage the equipment in accordance with Federal agency rules and procedures, and submit an annual inventory listing.

(3) When the equipment is no longer needed, the grantee or subgrantee will request disposition instructions from the Federal agency.

(g) *Right to transfer title.* The Federal awarding agency may reserve the right to transfer title to the Federal Government or a third part named by the awarding agency when such a third party is otherwise eligible under existing statutes. Such transfers shall be subject to the following standards:

(1) The property shall be identified in the grant or otherwise made known to the grantee in writing.

(2) The Federal awarding agency shall issue disposition instruction within 120 calendar days after the end of the Federal support of the project for which it was acquired. If the Federal awarding agency fails to issue disposition instructions within the 120 calendar-day period the grantee shall follow §18.32(e).

(3) When title to equipment is transferred, the grantee shall be paid an amount calculated by applying the percentage of participation in the purchase to the current fair market value of the property.

8. [REQUIRED] Identify the format and timing of ISA reports to the Buyer/Parent Department. Include the type of reports (e.g., progress or status, data, etc.), timing of reports (e.g., weekly, monthly, final) and the medium for submission of reports (e.g., e-mail, Excel spreadsheet, paper, telephone):

Reporting Schedule

Quarter/Annual Report	Reporting Period	Due Date	Reporting Instrument/Format
1st Quarter	Oct 1 – Dec 31, 2017	January 10, 2018	EOPSS financial report/Excel and EOPSS progress report/Word
			BJA Online Performance Measurement Tool (PMT) Report
2nd Quarter	Jan 1 – Mar 31, 2018	April 10, 2018	EOPSS financial report/Excel and EOPSS progress report/Word
			BJA Online Performance Measurement Tool (PMT) Report
3rd Quarter	Apr 1 – Jun 30, 2018	July 10, 2018	EOPSS financial report/Excel and EOPSS progress report/Word

Quarter/Annual Report	Reporting Period	Due Date	Reporting Instrument/Format
			BJA Online Performance Measurement Tool (PMT) Report
4th Quarter	Jul 1 – Sep 30, 2018	October 10, 2018	EOPSS financial report/Excel and EOPSS progress report/Word
			BJA Online Performance Measurement Tool (PMT) Report
5th Quarter-FINAL	Oct 1 – Dec 31, 2018	January 10, 2019	EOPSS financial report/Excel and EOPSS progress report/Word
			BJA Online Performance Measurement Tool (PMT) Report
Accounts Payable			EOPSS financial report/Excel and EOPSS progress report/Word
			BJA Online Performance Measurement Tool (PMT) Report

Reports Defined

All hard copies of quarterly financial and progress reports must be mailed and postmarked by the due date. Quarterly financial reports must include a copy of the CIW (warehouse) report for all cash and match expenditures.

9. Additional ISA Terms:

The following represent the Federal, Office of Grants and Research and Commonwealth general grant terms, as well as specific grant conditions. Note that some of the conditions do not pertain to the scope of services in this ISA, however, you must comply with all those conditions that are pertinent. **Note: Research related grant projects must respond to Section 6.**

Section : 1 Federal Grant Funds Sub-recipients

When receiving a grant award of federal funds administered by OGR, sub-recipients must comply with **three sets of *general* grant conditions**: (1) federal conditions; (2) state conditions; and (3) OGR conditions. These three sets of general conditions are discussed in this primary document.

Federal conditions are based on laws passed by Congress, regulations issued by the federal department making the funds available and published in the Code of Federal Regulations (CFR), and financial guidance documents also created by the federal department making the funds available. Additionally in most cases, there are requirements and conditions associated with a *specific* federal grant stream which are not conditions of receipt of federal funds in general.

State conditions are established in laws passed by the Massachusetts Legislature and in orders and rules established by the Governor, and are referenced in the contract sub-recipients are required to execute. These conditions are found in the pages attached to the Standard Contract.

OGR conditions outline the further administrative requirements for each grant award established by EOPSS and OGR. They are included in this document.

Section 2: Basic Federal Grant Conditions

The basic federal grant conditions that follow apply to all federal grants, regardless of the federal department making the funds available.

- Audit Requirement of Federal Funds
    - OMB Circular A-133 requirements apply to each non-profit organization, each institution of higher education, and local governments as a whole when they or one of their departments receives federal funds. Any non-profit organization, institution of higher education, or local government spending more than $500,000 in federal funds *from all sources* within a 12-month period must have an audit performed on the use of the funds. OGR defines the

12-month period as July 1 to June 30. The following webpage provides the full text of this basic federal grant requirement: http://www.whitehouse.gov/sites/default/files/omb/assets/a133/a133_revised_2007.pdf

- Data Universal Number System (DUNS) and Central Contractor Registration (CCR)
  - All subrecipients of federal funds must have a nine-digit DUNS number in order. For more information: 1-866-705-5711 or http://fedgov.dnb.com/webform.
  - All subrecipients of federal funds must maintain annual registration in the CCR database: www.sam.gov

- Transparency Act Reporting for Federal Funds
  - The Federal Funding Accountability and Transparency Act (FFATA) requires EOPSS to report on a federal website specific award and subrecipient identifying information for each award greater than $25,000 OGR makes with federal funds it received after October 1, 2010. Prior to receiving funds, each affected subrecipient must report certain information to OGR so that EOPSS can fulfill its FFATA reporting requirements. Data reported by EOPSS may be viewed at www.USASpending.gov.

- Cost Principles for Federal Grants to *State and Local Governments*
  - 2 CFR Part 225 (formerly known as OMB Circular A-87) requirements apply only to state and local government subrecipients. These regulations list and define general categories of costs that are both allowable and unallowable. Examples are included below.
    - The cost of alcoholic beverages is unallowable.
    - Costs incurred by advisory councils are allowable.
    - Audit costs are allowable.
    - Compensation costs are allowable so long as they are consistent with that paid for similar work in other activities of the local government.
    - Entertainment costs are unallowable.
    - Equipment costs are allowable with the prior approval of OGR. Equipment having a useful life of more than one year or a current per-unit fair market value of $5,000 or more must be tracked. When replacing equipment purchased with federal funds, the equipment to be replaced may be used as a trade-in or can be sold with the proceeds used to offset the cost of the replacement equipment. In addition, during the period of the contract with OGR, insurance on the equipment is allowable. Information required to be captured and recorded appears in **Attachment A, Question 7.**
    - Travel costs are allowable if pre-approved by OGR and if they are consistent with costs normally allowed in like circumstances for non-federally funded activities. The following webpage provides the full text of this basic federal grant requirement: http://www.whitehouse.gov/omb/fedreg/2005/083105_a87.pdf.
    - If a subrecipient uses grant funds to pay its employees, the subrecipient must maintain timesheets for work performed with the grant funds. Timesheets must show the hours worked and must be signed by the employee paid with the grant funds.

- Cost Principles for Federal Grants to *Non-Profit Organizations and Institutions of Higher Education* requirements apply only to the non-profit and higher education subrecipients. The CFRs referenced below list and define general categories of costs that are allowable and unallowable. The links below provide the full text of these two basic federal grant requirements.
  - 2 CFR Part 220 pertains to Educational Institutions (formerly known as OMB Circular A-21): http://www.whitehouse.gov/omb/fedreg/2005/083105_a21.pdf.
  - 2 CFR Part 230 pertains to Non-profit Organizations (formerly known as OMB Circular A-122): http://www.whitehouse.gov/omb/fedreg/2005/083105_a122.pdf.

- Nondiscrimination Requirements
  - If you receive federal funds, you must comply with, and you must require your subcontractors, if any, to comply with, all applicable statutorily-imposed nondiscrimination requirements, which may include the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. § 3789d); the Victims of Crime Act (42 U.S.C. § 10604(e)); the Juvenile Justice and Delinquency Prevention Act of 2002 (42 U.S.C. § 5672(b)); the Civil Rights Act of 1964 (42 U.S.C. § 2000d); the Rehabilitation Act of 1973 (29 U.S.C. § 794); the Americans with Disabilities Act of 1990 (42 U.S.C. §§ 12131-34); the Education Amendments of 1972 (20 U.S.C. §§ 1681, 1683, 1685-86); the Age Discrimination Act of 1975 (42 U.S.C. §§ 6101-07); Ex. Order 13279 (equal protection of the laws for faith-based and community organizations); and 28 C.F.R. pt. 38 (U.S. Department of Justice Equal Treatment for Faith-Based Organizations).

- Per Title VI of the Civil Rights Act of 1964 and the Omnibus Crime Control and Safe Streets Act of 1968, you must take reasonable steps to provide meaningful access for persons with limited English proficiency.

- In the event a Federal or State court or Federal or State administrative agency makes a finding of discrimination after a due process hearing on the grounds of race, color, religion, national origin, sex, or disability against a recipient of funds, you must forward a copy of the finding to the Office for Civil Rights, Office of Justice Programs and to EOPSS/OGR.

- In accordance with federal civil rights laws, you shall not retaliate against individuals for taking action or participating in action to secure rights protected by these laws.

- Human Subjects Protection (for research subrecipients only, see Addendum 1).

Section 3: Additional Federal Department-Dependent Grant Conditions

In addition to the basic federal grant conditions, each federal department that is the source of the funds may impose additional conditions. If you are awarded funds by OGR that originate from any of the federal departments listed below, you should be familiar with the text from each of the applicable links.

U.S. Department of Justice Funds

The U.S. Department of Justice offers a Financial Guide that presents grant requirements as defined by this federal agency. All subrecipients of these funds must adhere to these requirements.

- The webpage for the US DOJ Financial Guide is as follows: http://www.ojp.usdoj.gov/financialguide/index.htm.

  Pay particular attention to the sections on (1) matching or cost sharing, (2) allowable costs, (3) unallowable costs, (4) procurement under awards of federal assistance, (5) costs requiring prior approval, (6) equipment, and (7) retention and access requirements for records.

- If you receive DOJ grant funds, you may be required to comply with the regulatory requirement to develop, maintain on file, and submit for review to the Office for Civil Rights, Office of Justice Programs and to OGR an Equal Employment Opportunity Plan (EEOP). The url for DOJ's system for implementing this requirement is as follows: http://www.ojp.usdoj.gov/about/ocr/eeop_comply.htm

Section 4: Office of Grants and Research Conditions

In addition to the federal and state general grant conditions outlined above, the Office of Grants and Research (OGR) in the Executive Office of Public Safety and Security (EOPSS) has certain grant conditions that are essential to the administration of grant awards. Whether subrecipients are receiving funds from a federal or state grant, they must adhere to these conditions.

- **Federal *and* State Conditions** must be adhered to by subrecipients of federal grant funds.
- **Time extensions** of contracts, while uncommon, may be granted at the option of OGR. They are not encouraged or guaranteed.
  - If a subrecipient needs additional time to complete the scope of work for the grant award, OGR may grant a time-only extension as long as the revised contract containing the extension request is executed by both the subrecipient and OGR before the current end date of the contract. No time extension can be granted if the revised contract form is executed after the current end date of the contract.
  - Requests for time extensions must to be made at least 30 days before the end date of the contract.
- **Award amounts remaining at the end of the ISA/contract** will be reverted back to OGR. All goods must be received and all services rendered by the end date of the contract.
- **Each ISA has a defined accounts payable period. All payments must be made for services rendered or goods received by the end of this period.**
- **An ISA that crosses a state fiscal year (June 30) into the next fiscal year must observe the Commonwealth's policies on payment corrections or overpayments. That is, any mistakes in coding must be corrected with an EX transaction before August 31. All payroll corrections must be made by the date in July specified in the Fiscal Year Open/Close guidance issued each year by the Office of the State Comptroller. Any overpayments must be made corrected with an ER transaction before August 31.**
- **EPS certifies that the start date is the date the funds are loaded into MMARS and available to the child department.**
- **Programmatic and financial reports** must be received in accordance with the requirements of the specific award. At the option of OGR, reimbursement will be held until all reporting requirements are met.

- **Allowable grant-related travel costs** charged to grant awards will currently be paid at the lesser of $.45 per mile or the subrecipient's normal reimbursement rate. This rate is subject to change. Tolls and parking for grant-related local travel may also be paid. Receipts are required.
- **Indirect cost rates** will not be reimbursed based on a percentage rate without documentation of the rate having been approved by a federal agency. When a percentage rate has not been approved by a federal agency, a subrecipient may request of OGR allowable direct costs that will be incurred and can be specifically allocated to the project being funded.
- **Procurement practices** of subrecipient agencies must be followed. The subrecipient should ensure that its procurement practices conform to any specific federal guidelines found in the references in the federal conditions section above. Where there is a difference between the practices of the subrecipient agency/organization and a federal guideline, the more restrictive procedure applies.
- **Timesheets** must be maintained by subrecipients for work performed by its employee(s) paid for with grant funds. Timesheets must show the hours worked and paid for with grant funds and must be signed by the employee(s).
- **Submission of "Federal OMB Circular A-133 Audit Form**" is required for subrecipients that receive more than $500,000 in federal funds from all sources. OGR has developed a "self-identifying" form titled "Federal OMB Circular A-133 Audit Form" to be submitted to OGR at the end of the fiscal year and after the completion of an A-133 federal funds audit. The form asks if the subrecipient was required to have an audit and, if so, to identify any findings related to the federal funds awarded by OGR.
- **Site visits** to subrecipients will be made by OGR periodically. All records, papers, and other documents of any kind related to the funded activity must be made promptly available upon request for inspection and copying to any person authorized by OGR.
- **Grant-related documents** must be retained for a period of six years from the close of the contract.
- **Evaluations** of a subrecipient's funded program by an outside evaluator during or at the conclusion of the project period, should be reported to OGR in writing and a copy of the evaluation should be provided.
- **Reporting alleged fraud, waste or abuse** to the Office of the State Auditor or Inspector General and/or to an applicable federal agency is the responsibility of the subrecipient. This includes any alleged violations, serious irregularities, sensitive issues or overt or covert acts involving the use of public funds in a manner not consistent with federal statutes, related laws and regulations, appropriate guidelines, or purposes of the grant.
- **Use of funds should begin** within 60 days of the start of the contract, and if they are not, the subrecipient must report to OGR the steps taken to initiate the grant activities, the reasons for the delay, and the expected start of the use of the funds. If meaningful implementation steps have not begun after 60 days of the grant start date, OGR reserves the right to cancel the contract.
- **Subcontractors** implementing activities with grant funds must adhere to the grant provisions in this document and should be approved by OGR prior to subrecipients executing subcontracts.
- **Instructional materials** created or produced with grant funds will be "work made for hire," as defined in United States copyright law, and EOPSS shall be considered the author. EOPSS shall be the sole owner of all rights pertaining to these materials, including copyrights and all rights to use, reproduce, or publish the materials, and subrecipients may not use, reproduce, or distribute such materials without prior written approval of OGR. If a project results in the production of **other original books, manuals, or copyrightable material**, unless otherwise provided in the contract documents, EOPSS reserves a royalty-free, non-exclusive and irrevocable license to reproduce, publish, translate or otherwise use, and authorize others to publish and use, such material. If paid with federal funds, the grant number must appear on the materials.
- **Audio visual or written materials** developed as part of the grant may be required to incorporate specific language or disclaimers (e.g., regarding the federal source of funding) and in some instances pre-approval from the federal funding agency as instructed by the OGR grants manager.

Section 5: Additional OGR Conditions for Law Enforcement Agencies

Law enforcement agencies are subject to mandatory reporting requirements of various information, including, but not limited to the reporting requirements listed below. EOPSS and OGR may withhold reimbursements, cancel your contract, or withhold execution of any future grants for law enforcement agencies that do not comply with reporting requirements.

- ***Crime Data Reporting.*** Law enforcement organizations must submit timely and satisfactory monthly Uniform Crime Reporting (UCR) or National Incident Based Reporting System (NIBRS) reports to the Commonwealth's Crime Reporting Unit at the Commonwealth Fusion Center. <u>If your organization has hardware and software that support the creation of NIBRS data, crime data must be submitted to the Crime Reporting Unit in that format.</u>

- ***Motor Vehicle Accident Reporting.*** Police departments are required to report to the Registry of Motor Vehicles, within 15 days, accidents in which death, injury, or property damage in excess of $1,000 occurs (M.G.L. c. 90, § 29). The crash reports can be

delivered to the Registry of Motor Vehicles (RMV) main office through post office mail or through electronic submission. You may contact the RMV headquarters for any additional information.

- ***Juvenile Lockup Data.*** Law enforcement agencies that maintain a juvenile lockup must submit monthly juvenile lockup data to the Department of Criminal Justice Information Services via CJIS/LEAPS. Contact OGR's Juvenile Justice Program Coordinator for additional information.

- ***Fingerprint Cards.*** Law enforcement agencies must regularly submit fingerprint cards for all felony arrests to the Identification Section at the Massachusetts State Police Crime Lab as required by state law (M.G.L. c. 263, § 1A; G.L. c. 94C, § 45).

Section 6: Additional OGR Conditions for Research Grants Only: Human Subjects Protection

Research subrecipients must check one of the statements below.

[ ] a. The research activities covered under this Contract/ISA do not involve human subjects.
[ ] b. The research activities covered under this Contract/ISA do involve human subjects.

If the research activities involve human subjects (option b), then the subrecipient agrees to certify compliance with 28 C.F.R. Part 46 regulations by completing, “Protection of Human Subjects, IRB Certification, Declaration of Exemption (Common Rule).” This form is available at the National Institute of Justice webpage at http://www.ojp.usdoj.gov/nij/funding/humansubjects/human-subjects.htm

The regulation for The Protection of Human Subjects 28 C.F.R Part 46 section 46.101(b)(1-6) defines categories of research involving human subjects that are exempt from its provisions. Details on exemptions can be found at the same National Institute of Justice webpage listed above.

***SPECIFIC CONDITIONS for JAG Award* # 2016-DJBX-0653**

1. Applicability of Part 200 Uniform Requirements

The Uniform Administrative Requirements, Cost Principles, and Audit Requirements in 2 C.F.R. Part 200, as adopted and supplemented by the Department of Justice (DOJ) in 2 C.F.R. Part 2800 (the "Part 200 Uniform Requirements") apply to this 2016 award from the Office of Justice Programs (OJP). For this 2015 award, the Part 200 Uniform Requirements, which were first adopted by DOJ on December 26, 2014, supersede, among other things, the provisions of 28 C.F.R. Parts 66 and 70, as well as those of 2 C.F.R. Parts 215, 220, 225, and 230.

If this 2016 award supplements funds previously awarded by OJP under the same award number, the Part 200 Uniform Requirements apply with respect to all award funds (whether derived from the initial award or a supplemental award) that are obligated on or after the acceptance date of this 2015 award.

Potential availability of grace period for procurement standards: Under the Part 200 Uniform Requirements, a time limited grace period may be available under certain circumstances to allow for transition from policies and procedures that complied with previous standards for procurements under federal awards to policies and procedures that comply with the new standards (that is, to those at 2 C.F.R. 200.317 through 200.326).

For more information on the Part 200 Uniform Requirements, including information regarding the potentially-available grace period described above, see the Office of Justice Programs (OJP) website at http://ojp.gov/funding/Part200UniformRequirements.htm.

In the event that an award-related question arises from documents or other materials prepared or distributed by OJP that may appear to conflict with, or differ in some way from, the provisions of the Part 200 Uniform Requirements, the recipient is to contact OJP promptly for clarification.

2. The recipient agrees to comply with the Department of Justice Grants Financial Guide as posted on the OJP website (currently, the "2016 DOJ Grants Financial Guide").

3. The recipient acknowledges that failure to submit an acceptable Equal Employment Opportunity Plan (if recipient is required to submit one pursuant to 28 C.F.R. Section 42.302) that is approved by the Office for Civil Rights is a violation of the Standard

Assurances executed by the recipient, and may result in suspension of funding until such time as the recipient is in compliance, or termination of the award.

4. The recipient understands and agrees that OJP may withhold award funds, or may impose other related requirements, if the recipient does not satisfactorily and promptly address outstanding issues from audits required by the Part 200 Uniform Requirements (or by the terms of this award), or other outstanding issues that arise in connection with audits, investigations, or reviews of DOJ awards.

5. Recipient understands and agrees that it cannot use any federal funds, either directly or indirectly, in support of the enactment, repeal, modification or adoption of any law, regulation or policy, at any level of government, without the express prior written approval of OJP.

6. The recipient and any sub recipients must promptly refer to the DOJ OIG any credible evidence that a principal, employee, agent, sub recipient, contractor, subcontractor, or other person has -- (1) submitted a claim for award funds that violates the False Claims Act; or (2) committed a criminal or civil violation of laws pertaining to fraud, conflict of interest, bribery, gratuity, or similar misconduct involving award funds. Potential fraud, waste, abuse, or misconduct should be reported to the OIG by - mail: Office of the Inspector General U.S. Department of Justice Investigations Division 950 Pennsylvania Avenue, N.W. Room 4706 Washington, DC 20530 e-mail: oig.hotline@usdoj.gov hotline: (contact information in English and Spanish): (800) 869-4499 or hotline fax: (202) 616-9881 Additional information is available from the DOJ OIG website at www.usdoj.gov/oig

7. Restrictions and certifications regarding non-disclosure agreements and related matters

No recipient or subrecipient under this award, or entity that receives a contract or subcontract with any funds under this award, may require any employee or contractor to sign an internal confidentiality agreement or statement that prohibits or otherwise restricts, or purports to prohibit or restrict, the reporting (in accordance with law) of waste, fraud, or abuse to an investigative or law enforcement representative of a federal department or agency authorized to receive such information.

The foregoing is not intended, and shall not be understood by the agency making this award, to contravene requirements applicable to Standard Form 312 (which relates to classified information), Form 4414 (which relates to sensitive compartmented information), or any other form issued by a federal department or agency governing the nondisclosure of classified information.

1. In accepting this award, the recipient --

a. represents that it neither requires nor has required internal confidentiality agreements or statements from employees or contractors that currently prohibit or otherwise currently restrict (or purport to prohibit or restrict) employees or contractors from reporting waste, fraud, or abuse as described above; and

b. certifies that, if it learns or is notified that it is or has been requiring its employees or contractors to execute agreements or statements that prohibit or otherwise restrict (or purport to prohibit or restrict), reporting of waste, fraud, or abuse as described above, it will immediately stop any further obligations of award funds, will provide prompt written notification to the agency making this award, and will resume (or permit resumption of)such obligations only if expressly authorized to do so by that agency.

2. If the recipient does or is authorized to make subawards or contracts under this award --

a. it represents that --

(1) it has determined that no other entity that the recipient's application proposes may or will receive award funds (whether through a subaward, contract, or subcontract) either requires or has required internal confidentiality agreements or statements from employees or contractors that currently prohibit or otherwise currently restrict (or purport to prohibit or restrict) employees or contractors from reporting waste, fraud, or abuse as described above; and

(2) it has made appropriate inquiry, or otherwise has an adequate factual basis, to support this representation; and

b. it certifies that, if it learns or is notified that any subrecipient, contractor, or subcontractor entity that receives funds under this award is or has been requiring its employees or contractors to execute agreements or statements that prohibit or otherwise restrict (or purport to prohibit or restrict), reporting of waste, fraud, or abuse as described above, it will immediately stop any further obligations of award funds to or by that entity, will provide prompt written notification to the agency making this award, and will resume (or permit resumption of) such obligations only if expressly authorized to do so by that agency.

8. Recipient understands and agrees that it cannot use any federal funds, either directly or indirectly, in support of any contract or subaward to either the Association of Community Organizations for Reform Now (ACORN) or its subsidiaries, without the express prior written approval of OJP.

9. The recipient agrees to comply with any additional requirements that may be imposed during the grant performance period if the agency determines that the recipient is a high-risk grantee. Cf. 28 C.F.R. parts 66, 70.

10. The recipient agrees to comply with applicable requirements regarding registration with the System for Award Management (SAM) (or with a successor government-wide system officially designated by OMB and OJP). The recipient also agrees to comply with applicable restrictions on subawards to first-tier subrecipients that do not acquire and provide a Data Universal Numbering System (DUNS) number. The details of recipient obligations are posted on the Office of Justice Programs web site at http://www.ojp.gov/funding/sam.htm (Award condition: Registration with the System for Award Management and Universal Identifier Requirements), and are incorporated by reference here. This special condition does not apply to an award to an individual who received the award as a natural person (i.e., unrelated to any business or non-profit organization that he or she may own or operate in his or her name).

11. Pursuant to Executive Order 13513, "Federal Leadership on Reducing Text Messaging While Driving," 74 Fed. Reg. 51225 (October 1, 2009), the Department encourages recipients and sub recipients to adopt and enforce policies banning employees from text messaging while driving any vehicle during the course of performing work funded by this grant, and to establish workplace safety policies and conduct education, awareness, and other outreach to decrease crashes caused by distracted drivers.

12. The recipient agrees to comply with all applicable laws, regulations, policies, and guidance (including specific cost limits, prior approval and reporting requirements, where applicable) governing the use of federal funds for expenses related to conferences, meetings, trainings, and other events, including the provision of food and/or beverages at such events, and costs of attendance at such events. Information on rules applicable to this award appears in the DOJ Grants Financial Guide (currently, as section 3.10 of "Postaward Requirements" in the "2015 DOJ Grants Financial Guide").

13. The recipient understands and agrees that any training or training materials developed or delivered with funding provided under this award must adhere to the OJP Training Guiding Principles for Grantees and Subgrantees, available at http://www.ojp.usdoj.gov/funding/ojptrainingguidingprinciples.htm.

14.The recipient agrees that if it currently has an open award of federal funds or if it receives an award of federal funds other than this OJP award, and those award funds have been, are being, or are to be used, in whole or in part, for one or more of the identical cost items for which funds are being provided under this OJP award, the recipient will promptly notify, in writing, the grant manager for this OJP award, and, if so requested by OJP, seek a budget modification or change-of-project-scope grant adjustment notice (GAN) to eliminate any inappropriate duplication of funding.

15. The recipient understands and agrees that award funds may not be used to discriminate against or denigrate the religious or moral beliefs of students who participate in programs for which financial assistance is provided from those funds, or of the parents or legal guardians of such students.

16. The recipient understands and agrees that - (a) No award funds may be used to maintain or establish a computer network unless such network blocks the viewing, downloading, and exchanging of pornography, and (b) Nothing in subsection (a) limits the use of funds necessary for any Federal, State, tribal, or local law enforcement agency or any other entity carrying out criminal investigations, prosecution, or adjudication activities.

17. A recipient that is eligible under the Part 200 Uniform Requirements to use the "de minimis" indirect cost rate described in 2 C.F.R. 200.414(f), and that elects to use the "de minimis" indirect cost rate, must advise OJP in writing of both its eligibility and its election, and must comply with all associated requirements in the Part 200 Uniform Requirements. The "de minimis" rate may be applied only to modified total direct costs (MTDC).

18. The recipient must collect, maintain, and provide to OJP, data that measure the performance and effectiveness of activities under this award, in the manner, and within the timeframes, specified in the program solicitation, or as otherwise specified by OJP. Data collection supports compliance with the Government Performance and Results Act (GPRA) and the GPRA Modernization Act, and other applicable laws.

19. The recipient agrees to comply with OJP grant monitoring guidelines, protocols, and procedures, and to cooperate with BJA and OCFO on all grant monitoring requests, including requests related to desk reviews, enhanced programmatic desk reviews, and/or site visits. The recipient agrees to provide to BJA and OCFO all documentation necessary to complete monitoring tasks, including documentation related to any subawards made under this award. Further, the recipient agrees to abide by reasonable deadlines set by BJA and OCFO for providing the requested documents. Failure to cooperate with BJA's/OCFO's grant monitoring activities may result in sanctions affecting the recipient's DOJ awards, including, but not limited to: withholdings and/or other restrictions on the recipient's access to grant funds; referral to the Office of the Inspector General for audit review; designation of the recipient as a DOJ High Risk grantee; or termination of an award(s).

20. The recipient agrees to comply with applicable requirements to report first-tier subawards of $25,000 or more and, in certain circumstances, to report the names and total compensation of the five most highly compensated executives of the recipient and first-tier subrecipients of award funds. Such data will be submitted to the FFATA Subaward Reporting System (FSRS). The details of recipient obligations, which derive from the Federal Funding Accountability and Transparency Act of 2006 (FFATA), are posted on the Office of Justice Programs web site at http://www.ojp.gov/funding/ffata.htm (Award condition: Reporting Subawards and Executive Compensation), and are incorporated by reference here. This condition, and its reporting requirement, does not apply to grant awards made to an individual who received the award as a natural person (i.e., unrelated to any business or non-profit organization that he or she may own or operate in his or her name).

21. The recipient understands and agrees that it has a responsibility to monitor its subrecipients' compliance with applicable federal civil rights laws. The recipient agrees to submit written Methods of Administration (MOA) for ensuring subrecipients' compliance to the OJP's Office for Civil Rights at CivilRightsMOA@usdoj.gov within 90 days of receiving the grant award, and to make supporting documentation available for review upon request by OJP or any other authorized persons. The required elements of the MOA are set forth at http://www.ojp.usdoj.gov/funding/other_requirements.htm, under the heading, "Civil Rights Compliance Specific to State Administering Agencies."

22. In order to promote information sharing and enable interoperability among disparate systems across the justice and public safety community, OJP requires the grantee to comply with DOJ's Global Justice Information Sharing Initiative (DOJ's Global) guidelines and recommendations for this particular grant. Grantee shall conform to the Global Standards Package (GSP) and all constituent elements, where applicable, as described at: http://www.it.ojp.gov/gsp_grantcondition. Grantee shall document planned approaches to information sharing and describe compliance to the GSP and appropriate privacy policy that protects shared information, or provide detailed justification for why an alternative approach is recommended.

23. To avoid duplicating existing networks or IT systems in any initiatives funded by BJA for law enforcement information sharing systems which involve interstate connectivity between jurisdictions, such systems shall employ, to the extent possible, existing networks as the communication backbone to achieve interstate connectivity, unless the grantee can demonstrate to the satisfaction of BJA that this requirement would not be cost effective or would impair the functionality of an existing or proposed IT system.

24. Approval of this award does not indicate approval of any consultant rate in excess of $650 per day. A detailed justification must be submitted to and approved by the Office of Justice Programs (OJP) program office prior to obligation or expenditure of such funds.

25. All procurement (contract) transactions under this award must be conducted in a manner that is consistent with applicable Federal and State law, and with Federal procurement standards specified in regulations governing Federal awards to non-Federal entities. Procurement (contract) transactions should be competitively awarded unless circumstances preclude competition. Noncompetitive (e.g., sole source) procurements by the award recipient in excess of the Simplified Acquisition Threshold (currently $150,000) set out in the Federal Acquisition Regulation must receive prior approval from the awarding agency, and must otherwise comply with rules governing such procurements found in the current edition of the OJP Financial Guide.

26. The recipient agrees to participate in BJA-sponsored training events, technical assistance events, or conferences held by BJA or its designees, upon BJA's request.

27. The grantee agrees that within 120 days of award acceptance, each current member of a law enforcement task force funded with these funds who is a task force commander, agency executive, task force officer, or other task force member of equivalent rank, will

complete required online (internet-based) task force training. Additionally, all future task force members are required to complete this training once during the life of this award, or once every four years if multiple awards include this requirement. The training is provided free of charge online through BJA's Center for Task Force Integrity and Leadership (www.ctfli.org). This training addresses task force effectiveness as well as other key issues including privacy and civil liberties/rights, task force performance measurement, personnel selection, and task force oversight and accountability. When BJA funding supports a task force, a task force personnel roster should be compiled and maintained, along with course completion certificates, by the grant recipient. Additional information is available regarding this required training and access methods via BJA's web site and the Center for Task Force Integrity and Leadership (www.ctfli.org).

28. Award recipients must verify Point of Contact (POC), Financial Point of Contact (FPOC), and Authorized Representative contact information in GMS, including telephone number and e-mail address. If any information is incorrect or has changed, a Grant Adjustment Notice (GAN) must be submitted via the Grants Management System (GMS) to document changes.

29. Grantee agrees to comply with all confidentiality requirements of 42 U.S.C. section 3789g and 28 C.F.R. Part 22 that are applicable to collection, use, and revelation of data or information. Grantee further agrees, as a condition of grant approval, to submit a Privacy Certificate that is in accord with requirements of 28 C.F.R. Part 22 and, in particular, section 22.23.

30. Grantee agrees to comply with the requirements of 28 C.F.R. Part 46 and all Office of Justice Programs policies and procedures regarding the protection of human research subjects, including obtainment of Institutional Review Board approval, if appropriate, and subject informed consent.

31. The grantee agrees to comply with the applicable requirements of 28 C.F.R. Part 38, the Department of Justice regulation governing "Equal Treatment for Faith Based Organizations" (the "Equal Treatment Regulation"). The Equal Treatment Regulation provides in part that Department of Justice grant awards of direct funding may not be used to fund any inherently religious activities, such as worship, religious instruction, or proselytization. Recipients of direct grants may still engage in inherently religious activities, but such activities must be separate in time or place from the Department of Justice funded program, and participation in such activities by individuals receiving services from the grantee or a sub-grantee must be voluntary. The Equal Treatment Regulation also makes clear that organizations participating in programs directly funded by the Department of Justice are not permitted to discriminate in the provision of services on the basis of a beneficiary's religion. Notwithstanding any other special condition of this award, faithbased organizations may, in some circumstances, consider religion as a basis for employment. See http://www.ojp.gov/about/ocr/equal_fbo.htm.

32. The recipient agrees that any information technology system funded or supported by OJP funds will comply with 28 C.F.R. Part 23, Criminal Intelligence Systems Operating Policies, if OJP determines this regulation to be applicable. Should OJP determine 28 C.F.R. Part 23 to be applicable, OJP may, at its discretion, perform audits of the system, as per the regulation. Should any violation of 28 C.F.R. Part 23 occur, the recipient may be fined as per 42 U.S.C. 3789g(c)-(d). Recipient may not satisfy such a fine with federal funds.

33. Program income (as defined in the Part 200 Uniform Requirements) must be used in accordance with the provisions of the Part 200 Uniform Requirements. Program income earnings and expenditures both must be reported on the quarterly Federal Financial Report, SF 425.

34. Award recipients must submit quarterly a Federal Financial Report (SF-425) and annual performance reports through GMS (https://grants.ojp.usdoj.gov). Consistent with the Department's responsibilities under the Government Performance and Results Act (GPRA), P.L. 103-62, applicants who receive funding under this solicitation must provide data that measure the results of their work. Therefore, quarterly performance metrics reports must be submitted through BJA's Performance Measurement Tool (PMT) website (www.bjaperformancetools.org). For more detailed information on reporting and other JAG requirements, refer to the JAG reporting requirements webpage. Failure to submit required JAG reports by established deadlines may result in the freezing of grant funds and future High Risk designation.

35. The recipient agrees that funds received under this award will not be used to supplant State or local funds, but will be used to increase the amounts of such funds that would, in the absence of Federal funds, be made available for law enforcement activities.

36. The recipient agrees to monitor subawards under this JAG award in accordance with all applicable statutes, regulations, OMB circulars, and guidelines, including the OJP Financial Guide, and to include the applicable conditions of this award in any subaward. The recipient is responsible for oversight of subrecipient spending and monitoring of specific outcomes and benefits attributable to use

of JAG funds by subrecipients. The recipient agrees to submit, upon request, documentation of its policies and procedures for monitoring of subawards under this award.

37. The recipient agrees to submit a signed certification that that all law enforcement agencies receiving vests purchased with JAG funds have a written "mandatory wear" policy in effect. Fiscal agents and state agencies must keep signed certifications on file for any subrecipients planning to utilize JAG funds for ballistic-resistant and stab-resistant body armor purchases. This policy must be in place for at least all uniformed officers before any JAG funding can be used by the agency for body armor. There are no requirements regarding the nature of the policy other than it being a mandatory wear policy for all uniformed officers while on duty.

38. Ballistic-resistant and stab-resistant body armor purchased with JAG funds may be purchased at any threat level, make or model, from any distributor or manufacturer, as long as the vests have been tested and found to comply with applicable National Institute of Justice ballistic or stab standards and are listed on the NIJ Compliant Body Armor Model List (http://nij.gov). In addition, ballistic-resistant and stab-resistant body armor purchased must be American made. The latest NIJ standard information can be found here: http://www.nij.gov/topics/technology/body-armor/safetyinitiative. htm.

39. JAG funds may be used to purchase vests for an agency, but they may not be used as the 50% match for purposes of the Bulletproof Vest Partnership (BVP) program.

40. The recipient is required to establish a trust fund account. (The trust fund may or may not be an interest-bearing account.) The fund, including any interest, may not be used to pay debts or expenses incurred by other activities beyond the scope of the Edward Byrne Memorial Justice Assistance Grant Program (JAG). The recipient also agrees to obligate the grant funds in the trust fund (including any interest earned) during the period of the grant and expend within 90 days thereafter. Any unobligated or unexpended funds, including interest earned, must be returned to the Office ofJustice Programs at the time of closeout.

41. The grantee agrees to assist BJA in complying with the National Environmental Policy Act (NEPA), the National Historic Preservation Act, and other related federal environmental impact analyses requirements in the use of these grant funds, either directly by the grantee or by a subgrantee. Accordingly, the grantee agrees to first determine if any of the following activities will be funded by the grant, prior to obligating funds for any of these purposes. If it is determined that any of the following activities will be funded by the grant, the grantee agrees to contact BJA.

The grantee understands that this special condition applies to its following new activities whether or not they are being specifically funded with these grant funds. That is, as long as the activity is being conducted by the grantee, a subgrantee, or any third party and the activity needs to be undertaken in order to use these grant funds, this special condition must first be met. The activities covered by this special condition are:
a. New construction;
b. Minor renovation or remodeling of a property located in an environmentally or historically sensitive area, including properties located within a 100-year flood plain, a wetland, or habitat for endangered species, or a property listed on or eligible for listing on the National Register of Historic Places;
c. A renovation, lease, or any proposed use of a building or facility that will either (a) result in a change in its basic prior use or (b) significantly change its size;
d. Implementation of a new program involving the use of chemicals other than chemicals that are (a) purchased as an incidental component of a funded activity and (b) traditionally used, for example, in office, household, recreational, or education environments; and
e. Implementation of a program relating to clandestine methamphetamine laboratory operations, including the identification, seizure, or closure of clandestine methamphetamine laboratories.

The grantee understands and agrees that complying with NEPA may require the preparation of an Environmental Assessment and/or an Environmental Impact Statement, as directed by BJA. The grantee further understands and agrees to the requirements for implementation of a Mitigation Plan, as detailed at http://www.ojp.usdoj.gov/BJA/resource/nepa.html, for programs relating to methamphetamine laboratory operations.

Application of This Special Condition to Grantee's Existing Programs or Activities: For any of the grantee's or its subgrantees' existing programs or activities that will be funded by these grant funds, the grantee, upon specific request from BJA, agrees to cooperate with BJA in any preparation by BJA of a national or program environmental assessment of that funded program or activity.

42. BJA strongly encourages the recipient to submit annual (or more frequent) JAG success stories. To submit a success story, sign in to your My BJA account at https://www.bja.gov/Login.aspx to access the Success Story Submission form. If you do not yet have a My

BJA account, please register at https://www.bja.gov/profile.aspx. Once you register, one of the available areas on your My BJA page will be "My Success Stories". Within this box, you will see an option to add a Success Story. Once reviewed and approved by BJA, all success stories will appear on the new BJA Success Story web page at https://www.bja.gov/SuccessStoryList.aspx.

43. Recipient understands and agrees that award funds may not be used for items that are listed on the Prohibited Expenditure List at the time of purchase or acquisition, including as the list may be amended from time to time. The Prohibited Expenditure list may be accessed here: https://www.bja.gov/funding/JAGControlledPurchaseList.pdf.

44. Recipient understands and agrees that award funds may not be used for items that are listed on the Controlled Expenditure List at the time of purchase or acquisition, including as the list may be amended from time to time, without explicit written prior approval from BJA. The Controlled Expenditure List and instructions on how to request approval for purchase or acquisitions may be accessed here: https://www.bja.gov/funding/JAGControlledPurchaseList.pdf

45. Recipient understands and agrees that the purchase or acquisition of any item on the Controlled Expenditure List at the time of purchase or acquisition, including as the list may be amended from time to time, with award funds by an agency will trigger a requirement that the agency collect and retain (for at least 3 years) certain information about the use of 1) any federally-acquired Controlled Equipment in the agency's inventory, and 2) any other controlled equipment in the same category as the federally-acquired controlled equipment in the agency's inventory, regardless of source; and make that information available to BJA upon request. Details about what information must be collected and retained may be accessed here: https://www.whitehouse.gov/sites/default/files/docs/le_equipment_wg_final_report_final.pdf

46. Recipient understands and agrees that, notwithstanding 2 CFR § 200.313, no equipment listed on the Controlled Expenditure List that is purchased under this award may be transferred or sold to a third party, except as described below:

a. Agencies may transfer or sell any controlled equipment, except riot helmets and riot shields, to a Law Enforcement Agency (LEA) after obtaining prior written approval from BJA. As a condition of that approval, the acquiring LEA will be required to submit information and certifications to BJA as if it was requesting approval to use award fund for the initial purchase of items on the Controlled Expenditure List.
b. Agencies may not transfer or sell any riot helmets or riot shields purchased under this award.
c. Agencies may not transfer or sell any Controlled Equipment purchased under this award to non-LEAs, with the exception of fixed wing aircraft, rotary wing aircraft, and command and control vehicles. Before any such transfer or sale is finalized, the agency must obtain prior written approval from BJA. All law enforcement-related and other sensitive or potentially dangerous components, and all law enforcement insignias and identifying markings must be removed prior to transfer or sale.

Recipient further understands and agrees to notify BJA prior to the disposal of any items on the Controlled Expenditure List purchased under this award, and to abide by any applicable laws and regulations in such disposal.

47. Recipient understands and agrees that failure to comply with conditions related to Prohibited or Controlled Expenditures may result in a prohibition from further Controlled Expenditure approval under this or other federal awards.

48. Recipient acknowledges the final agency decision made by the U.S. Department of Justice that recipient's jurisdiction did not substantially implement the Sex Offender Registration and Notification Act (P.L. 109-248) before the deadline, which determination impacts the funding amount of this award, pursuant to 42 U.S.C. § 16925. In accepting this specific formula award, recipient hereby voluntarily agrees that if it elects to file a judicial appeal of that final agency decision, which was integral in determining this particular funding amount, no such appeal may commence more than 6 months after the date of this award.

49. With respect to this award, federal funds may not be used to pay cash compensation (salary plus bonuses) to any employee of the award recipient at a rate that exceeds 110% of the maximum annual salary payable to a member of the federal government's Senior Executive Service (SES) at an agency with a Certified SES Performance Appraisal System for that year. (An award recipient may compensate an employee at a higher rate, provided the amount in excess of this compensation limitation is paid with non-federal funds.)

This limitation on compensation rates allowable under this award may be waived on an individual basis at the discretion of the OJP official indicated in the program announcement under which this award is made.

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM
ATTACHMENT B - BUDGET

Check one: _X_ Initial ISA Budget

____ ISA Budget/Account Amendment. Maximum Obligation of ISA before this Amendment: $_____.

PRIOR MMARS DOCUMENT ID: _____ (for reference - if applicable)

CURRENT DOC ID: ISAEPSJG16HEROPOL18A.

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

A Budget Fiscal Year	B Seller/Child Account	C Object Class	D Description	E Initial ISA Amount / or Amount Prior to Amendment	F Indicate Add or Reduce +/-	G Amendment Amount	H Enter "YES" if Amount is a prior FY budget reduction or a current FY "Carry-in" authorization for Federal ISA Funds	I New Amount After Amendment
				$		$		$
				$		$		$
				$		$		$
				$		$		$
				$		$		$
				$		$		$
				$		$		$
				$		$		$
				$		$		$
				$		$		$
				$		$		$
				$		$		$

FISCAL YEAR SUBTOTALS AND TOTAL MAXIMUM OBLIGATION FOR DURATION OF ISA	
FISCAL YEAR: _2017_____ SUBTOTAL (*or New Subtotal if Fiscal Year Subtotal being amended*	$
FISCAL YEAR: __2018_____ SUBTOTAL (*or New Subtotal if Fiscal Year Subtotal being amended*	$
FISCAL YEAR: _____ SUBTOTAL (*or New Subtotal if Fiscal Year Subtotal being amended*	$
FISCAL YEAR: _____ SUBTOTAL (*or New Subtotal if Fiscal Year Subtotal being amended*	$
TOTAL MAXIMUM OBGLIGATON FOR DURATION OF ISA (*or New Total Maximum Obligation if amended*)	$97,946.80

Additional Budget Specifications:

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM
ATTACHMENT C – FEDERAL GRANT SELLER/CHILD ACCOUNT

[Complete ONLY if Buyer/Parent Account is a Federal Grant Account. Seller/Child Department must signoff in order to process document.]

__X__ NEW ISA ___ ISA AMENDMENT	**BUDGET FISCAL YEAR: 2018**
BUYER/PARENT DEPARTMENT: EPS	**SELLER/CHILD DEPARTMENT: POL**
CTR ONLY - REVENUE BUREAU WILL ASSIGN	
Revenue Budget	Revenue Source
BUYER/PARENT DEPARTMENT MUST COMPLETE ALL ITEMS BELOW	
CENTRAL BUDGET STRUCTURE (BGCN - BQ89)	
Appropriation Number: 80004611	Payroll Indicator : __X__ Yes ___ No
Budgetary Estimated Receipts $	BGCN Document Identification No.: ISAEPSJG16HEROPOL18A
COST ACCOUNTING STRUCTURE (BGRG- BQ88)	
Total Maximum Obligation of ISA: $97,946.80	BGRG Document Identification No.: ISAEPSJG16HEROPOL18A
MAJOR PROGRAM TABLE SET-UP	
Major Program (6 chars. or less): BJAG	Major Program Short Name (same as appropriation number): 80004611
Major Program Name: Byrne Justice Assistance Grant	
PROGRAM PERIOD TABLE SET-UP OR EXTENDED PROGRAM PERIOD	
Effective From Date: 05/22/2009	Effective To Date: 06/30/2020
Program Period: EPP	
Program Period Name: EPP	Program Period Short Name: EPP
PROGRAM TABLE SET-UP	
Effective From Date: 12/01/2017	Effective To Date: 01/31/2019
Program Name: FFY2015 BJAG HEROIN/OPIOID	Program Short Name: 80004611
Program Code: **(MUST START WITH "F" followed by up to 9 characters) FJG1HEOP16**	Sub Account: 2016-DJ-BX-0653

FUNDING PROFILE - FUNDING LINE		
Draw Name:	Customer ID	Payment System Code – **Check one option only**
EDCAPS:	VC7000000001	__**D**
ECHO:	VC7000000002	__**E**
LOCES:	VC7000000003	__**L**
SMARTLINK:	VC7000000004	__**S**
ASAP- OTHER:	VC7000000005	__**Y**
ASAP:	VC7000000006	__**Z**
GRANT- NON DRAW:	VC7000000007	__X__ **No Code**

FUNDING IDENTIFICATION	
Federal Catalog Agency: (2 digit code) 16	Federal Catalog Suffix: (3 digit code) **738**
Letter of Credit No.: 1504 1240	

Authorized Signatory Seller/Child Department: _____ Date:_____ Name: _____.

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM INSTRUCTIONS

The Interdepartmental Service Agreement (ISA) Form is issued by the Office of the Comptroller (CTR) pursuant to 815 CMR 6.00 for use by all Commonwealth Departments. The ISA Instructions are provided to assist both Buyer/Parent and Seller/Child Commonwealth Departments with the interpretation and completion of the ISA Form and are incorporated by reference into the ISA. The ISA Form is the "Contract" that documents the business agreement (joint venture) between two Commonwealth departments within the Executive, Judicial and Legislative Branches of government. A Department must be recognized as a Department in the State Accounting System (hereinafter referred to as "MMARS") in order to transfer or receive funding under an ISA. The ISA must comply with funding language in any appropriation act funding the ISA, as well as all applicable general and special state or federal laws, regulations. The Buyer/Parent and Seller/Child are responsible for reviewing and complying with the applicable CTR policies (including but not limited to the ISA, electronic signature and state finance law policies) located at the CTR Knowledge Center under Procurement and Contracts and also at the CTR Website at: Comptroller Policies. While reasonable efforts have been made to assure the accuracy of the legal requirements for ISAs, Departments should consult with their legal counsel to ensure compliance with all legal requirements related to their performance under an ISA. PLEASE NOTE THAT NOT ALL APPLICABLE LAWS HAVE BEEN CITED IN THIS DOCUMENT. INSTRUCTIONS AND HYPERLINKS MAY BE ADDED OR CHANGED WITHOUT NOTICE, SO CHECK THIS DOCUMENT PERIODICALLY FOR UPDATES.

➔ MMARS DOCUMENT ID: Enter the state accounting system (MMARS) BGCN or BGCS or other authorized MMARS document number associated with this ISA. ISA related DOC ID Numbering must be done as described below. The Doc ID must be the Doc ID entered into MMARS and reflected on the supporting ISA paperwork. All ISA Doc IDs MUST START WITH "ISA", as follows:

EXAMPLE DOC ID Number: **ISA**EPS12345678SDF06A

First 3 Characters	Second 3 Characters	Next 8 Characters	Next 3 Characters	Next 2 Characters*	Last Character
ISA	Buyer/Parent Department Alpha	Buyer/Parent defined. May be numeric, alpha or combination	Seller/Child Department Alpha	Fiscal Year	A (initial document) B (1st Amendment) C (2nd Amendment)
ISA	EPS	12345678	SDF	06	A

➔ BUDGET FISCAL YEAR. Enter the Budget Fiscal Year of the ISA or ISA Amendment, as appropriate.

➔ REQUEST FOR RESPONSE REFERENCE NUMBER. If the Seller/Child responded to an RFR that was posted on Comm-PASS, enter the RFR Reference Number as posted. If an RFR was not used, indicate "N/A". Seller/Child Departments may respond to a Request for Response (RFR) or other solicitation of a Buyer/Parent Department. If the Seller/Child Department is selected as a contractor, the ISA Form must be used as the "contract" (instead of the applicable Commonwealth Terms and Conditions and Standard Contract Form and Instructions).

➔ BUYER/PARENT/SELLER/CHILD DEPARTMENT NAME: Enter the 3 Alpha MMARS Department Code. For Example "CTR" for the Office of the Comptroller.

➔ BUSINESS MAILING ADDRESS: Enter the address where all correspondence to the ISA Manager must be sent. Unless otherwise specified in the ISA, legal notice sent or received by the Department's ISA Manager (with confirmation of actual receipt) through the listed fax number(s) or electronic mail address for the ISA Manager will meet any requirements for written notice under the ISA.

➔ ISA MANAGER: Identify the authorized ISA Manager who will be responsible for managing the ISA. ISA Managers must be Department Head Authorized Signatories in order to execute the ISA and otherwise obligate the Department with the appropriate MMARS Security to support Department Head Signature Authorization.

➔ PHONE/FAX/E-MAIL ADDRESS: Identify the phone, fax number(s) and electronic mail (e-mail) address of the ISA Manager.

➔ PURPOSE OF ISA. Check off whether this is a new ISA or an ISA Amendment. For New ISAs, enter the total Maximum obligation for the duration of the ISA. If an ISA Amendment, check off any of the Amendments that are being made and complete any information in the blanks provided and the Attachments that are identified.

➔ BRIEF DESCRIPTION OF PERFORMANCE GOALS TO BE ACCOMPLISHED BY THIS ISA, OR IF AMENDMENT, IDENTIFY WHAT IS BEING AMENDED: Identify a brief description of the ISA, ISA name and performance to be accomplished under the ISA. If an ISA Amendment, identify what is being amended. Merely stating "see attached" or referencing attachments without a narrative description of performance is insufficient *and will result in ISA or Amendment being returned to MMARS Liaison of Buyer/Parent Department*. The description is used to specifically identify the ISA performance, match the ISA with attachments and determine if the appropriate process has been selected.

➔ INDICATE WHETHER SELLER/CHILD DEPARTMENT STATE EMPLOYEES (AA OBJECT CLASS) WILL BE FULLY OR PARTIALLY FUNDED UNDER THIS ISA. Justification for use of state employees and details of who will be working and work that will be performed must be included as part of ATTACHMENT A.

➔ ACCOUNT INFORMATION.

- Check the correct option for either a BGCN – non-subsidiarized (federal, capital, trust); BGCS – subsidiarized (budgetary); Other (CT, RPO or other document authorized by CTR); Non-Financial ISA (no funds are transferred from Buyer/Parent to Seller/Child with resources committed to ISA; or Amendment without Budget changes to ISA (used only for an Amendment if there are no changes to the budget and no changes to Attachments B and C (if applicable).
- Identify for each account under the ISA whether the account is "added", "deleted or "no change". **THIS SECTION MUST BE COMPLETED FOR AMENDMENTS EVEN IF THE ACCOUNT INFORMATION HAS NOT CHANGED.** Enter each ISA account, fund, major program code and program code for all funding under the ISA. Attachment B must be completed for all financial ISAs and ISA Amendments (with Budgetary or Account amendments). Attachment C must be completed for any financial ISAs or ISA Amendments with Budgetary or Account amendments involving federal or capital funds).

➔ ISA ANTICIPATED START DATE**.** Enter the anticipated start date, provided that the Seller/Child certifies that it will not incur any obligations related to this ISA prior to the date that this ISA is executed, NOR prior to the date that sufficient funding for the obligations under this ISA available in the Seller/Child account for expenditure.
Note - ISA Duration. ISAs can be executed for the duration that makes sense from a business perspective. Multi-Year ISAs are encouraged if it best supports the Buyer/Parent and Seller/Child business processes. Similar to other types of contracts, all ISAs are subject to appropriation or other available funding. Therefore, Departments can enter into a Multi-year ISA even if funding transactions have to be

processed annually to support each fiscal year of the ISA. Buyer/Parent and Seller/Child Departments are responsible for ensuring that the funding is in place in the authorized Seller/Child account(s) to ensure that the Seller/Child Department can timely encumber funds and pay employees, contractors, grantees, etc. from the authorized ISA Seller/Child account(s)in accordance with the ISA Terms and Conditions.

➔ TERMINATION DATE OF THIS ISA: The Buyer/Parent Department must enter the date the ISA will terminate. An ISA must be signed for the full duration and amount in accordance with what is negotiated between the Buyer/Parent and Seller/Child Department. Amendments to extend the termination date, such as renewals, must be made using the ISA Form and must be signed by authorized Department Head signatories (with appropriate MMARS Authorized Signatory Security roles) of both the Buyer/Parent and the Seller/Child Department contemporaneously with the need for the amendment but no later than the termination date (or as previously amended) in accordance with 815 CMR 6.00.

➔ AUTHORIZING SIGNATURE FOR BUYER/PARENT DEPARTMENT/DATE: The Authorized Buyer/Parent Department Signatory must, in their own handwriting, and in ink, sign AND enter the date the ISA is signed. **THE DATE IS AN INEXTRICABLE PART OF THE SIGNATURE AND MUST BE COMPLETED BY THE SIGNATORY AND MAY NOT BE PRE-FILLED OR ENTERED AFTER THE SIGNATURE BY ANOTHER PERSON.** Rubber stamps, typed or other images are not acceptable. See CTR policies on Electronic Signature and Department Head Signature Authorization for Department Head and Authorized Signatory certifications and responsibilities.

➔ NAME /TITLE: The Buyer/Parent and Seller/Child Department Authorized Signatory's name and title must appear legibly.
NOTE: Secretariat signoff is not required in order for CTR to process an ISA. However, Seller/Child and Buyer/Parent Departments are required to follow any internal secretariat procedures when obtaining authorization for an ISA (or for certain ISA transactions such as an inter-subsidiary transfer "TS") prior to submission to CTR. All ISAs are periodically reviewed by CTR to verify that the signatories are authorized by their Department Head to execute contracts. Departments are responsible for timely processing through secretariats to ensure timely funding as required under the Department Head certifications.

➔ **ATTACHMENT A – TERMS OF PERFORMANCE AND JUSTIFICATIONS.** ***Attachment A is required for all new ISAs and for all ISA Amendments.*** Departments must use this attachment and insert (type, or copy and paste) the required information in addition to other terms of performance negotiated by the parties under Section 9. Sections 1-8 are mandatory and must be answered in detail or the ISA will be returned to the Buyer/Parent Department MMARS Liaison. All information must be inserted into Attachment A using as many pages as necessary. If Amending the ISA, completion of Sections 1, 2 and 3 identifying what is being amended and the reasons for the amendments is required. For sections 4-9 enter only the amended language in the sections being amended.

➔ **ATTACHMENT B - ANTICIPATED BUDGET.** ***Attachment B is required for all New ISAs and for all ISA Amendments with budget and accounting transactions.*** Departments must use this form. Insert all required information and use as many additional lines and pages as necessary. This attachment must breakdown the specifics of the ISA funding, by fiscal year, Seller/Child account, object class, description and amount. For multi-year ISAs the Attachment must provide a subtotal each fiscal year of the ISA (which equals each fiscal year's anticipated maximum obligation). All ISAs must provide a total maximum obligation for the total duration of the ISA (which must equal the total of all fiscal year subtotals) and must match the "Total Maximum Obligation for Duration of ISA" on the executed ISA.

- Check "Initial ISA Budget" , or "ISA Amendment"
- Identify the MMARS Doc ID if the ISA is being amended.
- **Complete Columns A-E For New ISAs. Complete Columns A-I for Amendments.**
  - **Column "A" (Budget Fiscal Year).** Enter the fiscal year of the funding, or amendment. For Multi year ISAs Column A must list planned expenditures by each fiscal year of the ISA.
  - **Column "B" (Seller/Child Account).** Enter the number of each Seller/Child account listed on the ISA Form. For ISAs using multiple Seller/Child Accounts, Column B must list planned expenditures for each Seller/Child account.
  - **Column "C" (Object Class).** Enter the Object Class (subsidiary) as outlined in the CTR Expenditure Classification Handbook (for example, "AA" for Employee compensation, "EE" for Administrative Expenses, "HH" for Consultant Contracts, etc.). IF the line item is authorized for multiple fiscal years, enter a separate line-item for each fiscal year of the ISA in which the line-item is authorized, specifying the estimated amount of the authorized expenditure. Line-items break downs of estimated expenditures by Object Class are required even if the Buyer/Parent account is non-subsidiarized, since the Budget acts as the authorization for the ISA expenditures. For subsequent fiscal years, entering "Balance Forward Amount" for federal, bond and trust accounts is insufficient, since good project management practices presume that departments will be managing estimated expenditures over the life of a project with planned fiscal year obligations, rather than managing projects solely based upon remaining uncommitted estimated receipts or uncommitted balances.
  - **Column "D" (Description).** Enter a brief description of the type of authorized budget expenditure or category, (e.g., "Conference Materials", "Program Manager", "Health Evaluations" etc.)
  - **Column "E" (Initial ISA Amount/or Amount Prior to Amendment).** Enter the amount for the budget item authorized under the ISA for each fiscal year. If the ISA is being amended, enter the current amount for this line-item, prior to the amendment. The Amendment amount will be entered in Column G and the new total will be entered in Column I.
  - **Column "F" (+/-)** is only used if the ISA is being amended to add or reduce a budget line item. Enter "+" for budget addition or "-" for a budget reduction.
  - **Column "G" Amendment Amount** is only used if the ISA is being amended to add or reduce a budget line item. Enter the amount of the budget line being increased or decreased.
  - **Column "H" (Carry-In)** is only used if the ISA is being amended to reduce a prior year federal grants fund line item with uncommitted estimated receipts that are being re-authorized in the current or a future fiscal year. Enter "YES" in this column for each line item being amended (by object class and description) to reflect a reduction in the budget in a prior fiscal year line item, and for each line item being added (by object class and description) to reflect a reauthorization of the funds in the current or a future fiscal year.
  - **Column "I" New Amount After Amendment** is only used if the ISA is being amended to add or reduce a budget line item. Enter new ISA Amount after the adding or reduction of the line-item amount referenced in Column G.
- FISCAL YEAR SUBTOTALS AND TOTAL MAXIMUM OBLIGATION.



- Fiscal Year Subtotals. For single fiscal year ISAs enter the fiscal year (e.g., "Fiscal Year 2007") and enter the subtotal of all "Current Amounts" (Column E) for that fiscal year. For Multi-year ISAs, enter each fiscal year of the ISA as a separate subtotal and enter the subtotal of all "Current Amounts" for each fiscal year.
- Total Maximum Obligation for Duration of ISA. Enter the Total Maximum Obligation for the Duration ISA for all fiscal years (as identified on the executed ISA Form). For single fiscal year ISAs, this amount should be the same as the Fiscal Year Subtotal. For Multi-fiscal year ISAs, this amount should equal the total of all the listed fiscal year subtotals.

➔ **ATTACHMENT C – FEDERAL GRANT SELLER/CHILD ACCOUNT** (complete only if Buyer/Parent Account is a Federal Account). Please enter the following information on this form.

- Enter whether this is a "New" ISA or an ISA Amendment and enter the Budget fiscal year.
- Enter the Buyer/Parent and Seller/Child Departments, which must match the ISA.
- *Skip the Revenue Budget and Revenue Source which will be completed by CTR.*
- CENTRAL BUDGET STRUCTURE*:*
  - Appropriation Number. Enter the Appropriation Number assigned by ANF.
  - Payroll Indicator. Enter a Payroll indicator of Yes or No.
  - Estimated Budgetary Receipts. Enter the amount of the Estimated Budgetary Receipts (the amount estimated in the ISA or Amendment for the current state fiscal year).
  - BGCN Document Identification No. Enter the MMARS Document Identification Number for the Central Expense Document (BGCN). The BGCN must be entered and submitted to PEND in MMARS. Providing a screen print of the BGCN aids CTR in the processing of the ISA and set up of the accounts or account changes.
- COST ACCOUNTING STRUCTURE.
  - Total Maximum Obligation of ISA or ISA Amendment Amount. For New ISAs, enter the Total Maximum Obligation of the ISA for the full duration of the ISA. For ISA Amendments, enter the amount of the modification.
  - BGRG Document Identification No. Enter the MMARS Document Identification Number for the Reimbursable Grant Budget Document (BGRG). The BGRG must be entered and submitted to PEND in MMARS. Providing a screen print of the BGRG aids CTR in the processing of the ISA and set up of the accounts or account changes.
- MAJOR PROGRAM TABLE SET-UP. This sets up the cost accounting hierarchy with groups of activities (programs) all part of one structure. For example – a major program could be wastewater management – WASTE. All documents (contracts, encumbrances, payments will reference this code.) All documents (contracts, encumbrances, payments will reference this code.)
  - Major Program. Enter the 6 (or fewer) character Major Program Code assigned by the department.
  - Major Program Name. Enter the full Major Program Name.
  - Major Program Short Name. Enter the Major Program Short Name.
- PROGRAM PERIOD TABLE SET-UP OR EXTENDED PROGRAM PERIOD (EPP). Enter the Program Period or Extended Program Period (EPP) information. This establishes the effective period of the grant. Please note that end dates are "hard edited" by the system, thus please take into account the accounts payable period for grants when establishing this date. Multiple periods allow for easy periodic reporting aligned to federal reporting dates. However, a Buyer/Parent department may choose to use 1 reporting period – EPP – that encompasses all dates. The downside of this method is that specific periodic federal reporting by the system is not achieved.
  - Enter the Program Effective From Date and Effective to Date.
  - Enter the Program Period or Extended Program Period (EPP) information.
  - Enter the Program Period Name, and Program Period Short Name.
- PROGRAM TABLE SET-UP.
  - Enter Program Name. For example a program could be for "storm water discharge".
  - Enter Program Short Name:
  - Program Code. Enter the 10 (or fewer) characters. All Federal Program codes must begin with the letter "**F"**. This is the second level of the cost accounting hierarchy. Programs are individual activities within a Major Program. Using the major program example, a program could be for storm water discharge – the program code would be "Fstormdis". All documents (Recurring Payment Order (RPO), payments will reference this code.)
  - The sub account must be the sub account in the award letter or the draw on the federal grant will fail. If a sub-account changes, this code must change.
- FUNDING PROFILE - Funding Line. This must be filled out properly – indicating the federal payment system to be used. If the wrong payment system is indicated, the draws on the federal grant will fail. Enter a check next to appropriate Payment System Code.
- FUNDING IDENTIFICATION.
  - Federal Catalog Agency Code. Enter the 2 digit Federal Catalog Agency code.
  - Federal Catalog Suffix. Enter the 3 digit Federal Catalog Suffix code from your award letter or contact the appropriate agency. This must align to the grant award. The proper grant identification information is a federal reporting requirement.
  - Letter of Credit No. Enter the Letter of Credit No. for this grant award.

COMPLETED ISAS SHOULD BE SUBMITTED FOR PROCESSING TO:

Office of the Comptroller, One Ashburton Place – 9th Floor, Attention: Accounts Payable Bureau, Contracts, Boston, MA 02108
CTR Helpline: **617-973-2468**

HOUSE DOCKET, NO. 1740 FILED ON: 1/19/2017

HOUSE . . . . . No. 1902

The Commonwealth of Massachusetts

PRESENTED BY:

William M. Straus

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act relative to license plate readers.

PETITION OF:

NAME:	DISTRICT/ADDRESS:
William M. Straus	*10th Bristol*

HOUSE DOCKET, NO. 1740 FILED ON: 1/19/2017

HOUSE . . . . . No. 1902

By Mr. Straus of Mattapoisett, a petition (accompanied by bill, House, No. 1902) of William M. Straus relative to license plate readers. Transportation.

The Commonwealth of Massachusetts

In the One Hundred and Ninetieth General Court
(2017-2018)

An Act relative to license plate readers.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. The General Laws, as appearing in the 2014 Official Edition, are hereby amended by inserting after chapter 90I the following chapter:-

Chapter 90J Automatic License Plate Reader Systems

Section 1. Definitions

As used throughout this chapter, the following words shall have the following meanings:

"ALPR data" means any data captured, created or originated by an ALPR system, including, without limitation, GPS coordinates, dates, times, images and license plate numbers, existing in an any form or medium, whether electronic, paper or otherwise, and any copies thereof;

"Automated license plate reader system" or "ALPR system" means an automated system of one or more mobile or fixed high-speed cameras combined with computer algorithms to convert images of license plates into computer-readable data;

“Department” means department of transportation;

“Executive office” means executive office of public safety and security;

“Governmental entity” means any official, officer, agency, office, instrumentality, department, division, committee, board, advisory board, commission or other body or authority of the commonwealth, or of any county or municipality, or any employee thereof, or any agent or other person acting on behalf thereof while acting within the scope of such agency or representation;

“Law enforcement agency” means any state or municipal law enforcement agency;

“Law enforcement officer" means a state or municipal police officer or traffic or parking enforcement officer;

"Legitimate law enforcement purpose" means: detection or investigation of a crime, traffic violation or parking violation; operation of AMBER alerts; or searches for missing or endangered persons;

“Non-governmental entity” means any person other than a governmental entity;

“Person” means any individual, partnership, corporation, association, society, entity or governmental entity;

"Preservation request" means written notice delivered by a federal, state or municipal law enforcement agency or a defendant in a criminal case to the executive office or a non-governmental entity requesting that certain ALPR data be preserved and retained for a specified period of time not to exceed 30 days from the date such request is received; provided, that such preservation request shall be accompanied by an affidavit stating: (i) the parameters identifying which ALPR data must be preserved, including, without limitation, the license plate numbers, if any, and the dates, times, and locations; and (ii) that such specified period of time is necessary to obtain a search warrant or production order compelling the production of such ALPR data; provided further, that the agency or defendant may serve subsequent preservation requests pending resolution of any motion filed in connection with such search warrant or production order, or any appeal related thereto;

"Production order" means an order or summons obtained by a defendant in a criminal case charged with a felony requiring a non-governmental entity or the executive office to produce ALPR data; provided, that such order or summons shall be issued in compliance with Massachusetts Rule of Criminal Procedure 17(a)(2); provided further, that any ALPR data produced in response to such order or summons shall be deemed privileged for the purposes of complying therewith;

"Search warrant" means: (i) a federal search warrant issued upon a determination of probable cause by a court or justice authorized to issue warrants in criminal cases that meets the requirements of the Federal Rules of Criminal Procedure; or (ii) a state search warrant issued pursuant to the requirements of sections 2 through 3A, inclusive, of chapter 276 by a court or justice authorized to issue warrants in criminal cases.

Section 2. State or municipal government; permitted uses

Notwithstanding any general or special law or regulation to the contrary, it shall be unlawful for any governmental entity to use an ALPR system; provided, however, that an ALPR system may be used by:

(a) law enforcement agencies for legitimate law enforcement purposes; and

(b) the department or an agent acting on behalf thereof for the purpose of assessing or collecting tolls or parking fees.

Section 3. General obligations

(a) Any database or other information against which license plate numbers are cross-referenced by an ALPR system operated by any person shall be updated every 24 hours, or at such other intervals as updated information become available if greater than 24 hours.

(b) Prior to taking any action in response to an alert or prompt from an ALPR system operated by any person, the individual so alerted shall confirm that the license plate number and state of issuance of the targeted vehicle matches the license plate number and state of issuance that prompted the alert.

Section 4. ALPR data; retention by law enforcement

Notwithstanding any general or special law or regulation to the contrary, not later than 48 hours following the time ALPR data is captured, created or originated by an ALPR system operated by a law enforcement agency, the law enforcement agency:

(a) may, at the option of the law enforcement agency, transfer such data to the executive office; and

(b) in any event shall permanently erase or destroy any such data in its possession, custody or control.

Section 5. ALPR data; retention by the executive office

(a) The executive office shall retain and store ALPR data transferred to it pursuant to section 4 for a period of 120 days. At the end of such 120-day period, the executive office shall permanently erase or destroy all such data in its possession, custody, or control.

(b) ALPR data may be retained beyond the 120-day period established under subsection (a) as necessary to comply with a search warrant, production order, or preservation request.

Section 6. ALPR data; retention by non-governmental entities

A governmental entity shall not enter into a business agreement with, or access ALPR data from, a non-governmental entity that retains ALPR data derived from vehicles registered or operated within the Commonwealth for periods longer than those established for the executive office under section 5.

Section 7. ALPR data; government access and review

Notwithstanding any general or special law or regulation to the contrary, a governmental entity may not access, search, review, disclose, or exchange ALPR data from any source; provided, however, that:

(a) a law enforcement agency or officer may access, search or review ALPR data as necessary to comply with section 3;

(b) a law enforcement agency, the executive office or the department, or an agent thereof, may access ALPR data as necessary to install, maintain or repair an ALPR system or a system storing ALPR data;

(d) a governmental entity may access, search, review or disclose ALPR data as necessary to respond to a reasonable belief that an individual is at imminent risk of serious physical injury, death or abduction; provided, that not later than 48 hours after accessing such ALPR data, the agency, executive office or department shall provide written notice to the office of the attorney general describing with particularity the grounds for such emergency access and the parameters of the ALPR data accessed, searched, reviewed or disclosed; provided further, that such ALPR data within the possession, custody or control of the law enforcement agency shall be permanently erased or destroyed not later than 48 hours after such imminent risk ceases to exist;

(e) a law enforcement agency or the executive office may access, search, review or disclose ALPR data as necessary to comply with: (i) sections 5 or 7; or (ii) a search warrant, production order or preservation request issued in connection with the investigation or prosecution of a felony;

(g) a law enforcement agency, a district attorney's office or the office of the attorney general may access, search, review or disclose ALPR data obtained pursuant to a production order or search warrant in order to further the investigation or prosecution of a felony; provided, that notwithstanding sections 4 and 5, such data may be retained until and shall be permanently

erased or destroyed promptly following the conclusion of the investigation or prosecution, including any appeals; or

(h) a governmental entity or an agent thereof may access, search, review or disclose ALPR data for the purpose of assessing, collecting or pursuing tolls, parking fees, or fines related to parking or traffic violations.

Section 8. Additional protections

Notwithstanding any general or special law or regulation to the contrary, ALPR data derived from vehicles registered or operated within the commonwealth shall not be used in any way by any person:

(i) to determine a person's numerical or other credit rating;

(ii) to determine whether to offer or enter into any secured or unsecured credit facility or loan;

(iii) to determine a person's insurance rate or rating with respect to any form of insurance, including, without limitation, any policy of life insurance, health insurance, automobile insurance or liability insurance; provided however, that nothing in this subsection shall be construed to prevent the verification of the accuracy of information submitted by an applicant to a motor vehicle insurance carrier or its agent in support of an application for or renewal of a motor vehicle insurance policy in order to make a determination as to whether to extend such insurance coverage;

(iv) to make any determination with respect to hiring, dismissal, discharge, suspension, compensation or any other employment decision; or

(v) to identify targets of or to engage in any form of promotion, marketing, advertising or solicitation.

Nothing in this section shall be construed to prevent a person from reporting unpaid tolls, violations or parking fees to any credit reporting agency.

Section 9. ALPR data; admissibility

(a) Notwithstanding any general or special law or regulation to the contrary, ALPR data produced, obtained or maintained in knowing violation of this chapter shall not be admitted, offered or cited by any governmental entity for any purpose in any criminal, civil, or administrative proceeding.

(b) Notwithstanding any general or special law or regulation to the contrary, ALPR data shall not be discoverable, admissible in evidence or offered or cited for any purpose in any civil or administrative proceeding by any party; provided, however, that subject to subsection (a), such data shall be admissible when offered in any civil or administrative proceeding (i) relating to the collection of tolls, parking fees, or traffic or parking violations, or (ii) arising out of claims of insurance fraud, motor vehicle theft, or motor vehicle repossession.

Section 10. Civil actions

(a) Any aggrieved person may institute a civil action in district or superior court for damages resulting from a violation of this chapter, or in superior court to restrain any such violation. If in any such action a willful violation is found to have occurred, the violator shall not be entitled to claim any privilege absolute or qualified, and he shall, in addition to any liability for such actual damages as may be shown, be liable for treble damages, or, in the alternative,

exemplary damages of not less than one hundred and not more than one thousand dollars for each violation, together with costs and reasonable attorney's fees.

(b) A violation of section 8 of this chapter shall also be a violation of section 2 of chapter 93A.

Section 11. Further regulation by governmental entities

Nothing contained in this chapter shall be construed to prevent a law enforcement agency, a municipality, the executive office or the department from adopting stricter limitations with respect to ALPR systems or ALPR data.

Section 12. Reporting

On or before March 1 annually, the executive office shall file a report with the clerks of the senate and house of representatives containing the following information based on data from the prior calendar year: (i) the total number of ALPR systems being operated within the commonwealth; (ii) the number of municipalities submitting ALPR data to the executive office pursuant to section 5; (iii) the number of license plate scans transferred to the executive office pursuant to section 5; and (iv) the number of search warrants and production requests seeking ALPR data served on the executive office.

Section 13. Executive office; rules and regulations

The executive office shall promulgate rules and regulations necessary to implement sections 2 through 7, inclusive, and section 12, including, without limitation, rules and regulations establishing an auditing process to assess compliance with this chapter by governmental entities.

Section 14. Office of the attorney general; enforcement

The attorney general shall enforce sections 2 through 8, inclusive, and shall have the power to petition the court for injunctive relief, relief under chapter 93A, or other appropriate relief against any person that fails to comply therewith.

Section 15. Severability

If any provision of this chapter or the application thereof to any person or circumstance is held invalid, the invalidity shall not affect other provisions or applications of the chapter which can be given effect without the invalid provision or application, and to this end the provisions of this chapter are declared to be severable.

Bureau of Justice Assistance
U.S. Department of Justice

License Plate Reader

Policy Development Template



For Use in **Intelligence and Investigative Activities**

February 2017

Where to Locate This Resource

This resource is available online at www.it.ojp.gov/privacy and at www.ncirc.gov. To request printed copies, send requests to information@ncirc.gov.

To Request a Word Version of the Template

To request a Word version, send requests to information@ncirc.gov.

This project was supported by Grant Number 2013-D6-BX-K001, awarded by the Bureau of Justice Assistance, in collaboration with the U.S. Department of Homeland Security. The Bureau of Justice Assistance is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice or the U.S. Department of Homeland Security.

License Plate Reader Policy Development Template for Use in Intelligence and Investigative Activities

February 2017



Table of Contents

Introduction **1**

A. License Plate Reader (LPR) Policies **2**

B. How to Use This Template **3**

C. Resource List **4**

License Plate Reader (LPR) Policy Development Template for Use in Intelligence and Investigative Activities **5**

A. Purpose Statement **5**

B. Policy Applicability and Legal Compliance **6**

C. Governance and Oversight **7**

D. Definitions **8**

E. Acquiring and Receiving LPR Information **8**

F. Use of LPR Information **11**

G. Sharing and Dissemination of LPR Information **12**

H. Information Quality Assurance **12**

I. Redress **14**

I.1 Disclosure 14

I.2 Corrections 14

I.3 Appeals 14

J. Security and Maintenance **15**

K. Information Retention and Purging **16**

L. Accountability and Enforcement 17

L.1 Transparency 17

L.2 Accountability 18

L.3 Enforcement 18

M. Training 19

Appendix A—Glossary of Terms and Definitions 21

Appendix B—Fair Information Practice Principles (FIPPs) 27

Appendix C—Listing of Federal Laws 31

Appendix D—Cases and Authorities 35

Appendix E—Sample LPR Policy 41

Introduction

Automatic license plate readers (ALPRs)—also known as license plate readers (LPRs)—use image-processing technology to identify vehicles by their license plates. LPRs automate a process that, in the past, was conducted manually by officers, license plate by license plate, with much officer discretion. Using a special form of optical character recognition (OCR), the LPR's algorithms transform pixels of a digital image into the text of a license plate. Since entering the market, LPRs have been employed in many applications, but one of the fastest-growing uses is by justice entities who use LPR technology as an investigative tool to aid them in recovering stolen vehicles, locating possible criminals, assisting in the security of large public venues, and conducting other intelligence and investigative activities. Images are captured by LPRs and translated into letters and numbers and compared to law enforcement databases of registered vehicles, including those known to be or suspected of being involved with crimes or infractions. If a match to possible criminal activity is found, the LPR system provides an alert to the officer that a suspected vehicle is in the immediate area of an LPR.

Through this growing adoption of LPRs, justice entities are reporting increased successes in locating stolen vehicles and identifying suspects. Dale Stockton, Program Manager, Road Runner, Automated Regional Justice Information System, San Diego, shared the following with attendees at a National Institute of Justice conference:

> This is the best tool we've had come along in a very long time. It can really impact crime. It can really impact public safety. . . . And, although it's often used for locating stolen cars, the reality is . . . the value goes far beyond stolen cars, particularly in the area of investigative support. . . . The biggest reason that we want to use LPR in the field, though, is that it truly is a force multiplier. Officers can do their normal job on patrol and the license plate reader functions in the background while the officer pays attention to what's going on around them. . . . One of the more recently realized applications is in support of homeland security because, around this country, we have identified infrastructure that we know is at risk . . . so if we start looking at vehicles frequenting that infrastructure, that can give us greater insight as to where potential risks are.[1]

News stories, like the ones listed below, are increasing, demonstrating the kinds of success justice entities have had in using LPRs:

- "A Look at Plate Readers That Helped Officer Catch Murder Suspect in West Carthage," WWNYTV 7, July 3, 2016.
- "Suspect in a Hit-and-Run Death of 9-Year-Old Girl Located Using Historical and Commercial License Plate Reader Data," PR Newswire, Livermore, California, March 31, 2016.
- "License Plate Readers Used to Find Journalist Killer Also Used in WNY," WIVB News Channel 4, Buffalo, New York, August 27, 2015.
- "Queens Man Pleads Guilty to Manslaughter in Death of Roommate's Friend," Office of Richard A. Brown, District Attorney, Queens County, New York, November 4, 2011.

"This is a great tool for us," said a New York State Trooper in an interview on license plate readers used to locate a suspect in shooting deaths of two journalists. "If it was a suspended plate, an alarm would go off on here saying registration suspected or revoked, and at that point in time I would have to make sure the plate that was read is the correct plate . . . . It is a great tool for law enforcement; it's a great tool for the community."[2]

[1] National Institute of Justice (NIJ) Audio Transcript: Using License Plate Readers to Fight Crime, www.nij.gov.
[2] "License Plate Readers Used to Find Journalist Killer Also Used in WNY," George Richert, News 4 Reporter, WIVB News Channel 4, Buffalo, New York, August 27, 2015, http://wivb.com/2015/08/27/license-plate-readers-found-virginia-suspect/.

Even with the proven efficacy of this technology, justice entities should be alert to risk of erroneous or deficient LPR data:

- "Driver Finds Himself Surrounded by Cops With Guns Out After Automatic License Plate Reader Misreads His Plate," TechDirt, April 28, 2014.
- "License Plate Reader Error Leads to Traffic Stop at Gun Point, Court Case," Ars Technica, May 12, 2014.

Justice entities should therefore put in place appropriate policies and procedures to guard against possible errors and other potential problems. Strong control and oversight are critical considerations in policy development, especially as the civil liberties implications of possible unforeseen derivative uses may be significant. Such efforts will not only enhance mission effectiveness but also safeguard privacy, civil rights, and civil liberties of individuals.

A. License Plate Reader (LPR) Policies

As illustrated by the successes described earlier, justice entities (such as law enforcement or homeland security agencies, fusion centers, and intelligence units) are turning to LPR technology more and more. However, when considering or implementing an LPR program, individual privacy, civil rights, and civil liberties must also be vigorously protected. Establishing and implementing such protections in an entity's LPR policy will help guide the justice entity's LPR information collection, receipt, access, use, dissemination, retention, and purging efforts. Such proactive work supports and enhances the justice entity's ability to both fulfill its mission while also protecting the privacy, civil rights, and civil liberties of community members—strengthening trust and public confidence through effective and responsible use of LPR technology.

When an entity determines to develop and implement an LPR policy, it is important to note that such a policy is not a one-time project; it is one component of an ongoing LPR program that works to protect privacy, civil rights, and civil liberties. As agencies consider establishing and implementing a policy for LPR information, they are encouraged to consider the LPR policy as one in a series of the following steps:

1. Educate and raise awareness on the importance of having privacy, civil rights, and civil liberties protections.
2. Assess agency privacy, civil rights, and civil liberties risks by evaluating the process through which the agency collects, receives, accesses, uses, disseminates, retains, and purges LPR information.
3. **Develop an LPR policy** to articulate the legal framework and policy position on how the agency handles LPR information.
4. Perform a policy evaluation, prior to publishing, to determine whether the policy adequately addresses current standards, privacy protection recommendations, and the law.
5. Implement and train personnel and authorized users on the established rules and procedures.
6. Perform an annual policy review and make appropriate changes in response to implementation experience, guidance from oversight or advisory bodies, applicable law, technology, and public expectations.
7. Audit the processes described in the LPR policy.

A comprehensive LPR policy that is developed in a transparent manner and properly enforced fosters trust—not only within and between justice partners but also by the public, whose LPR information may be collected and utilized. This process thus ensures that justice entities are serving as responsible stewards of LPR information and operating with respect for individual privacy and the law. Without this trust, LPR program initiatives may give rise to additional public scrutiny and civil liability.

To support justice entities in their efforts to implement LPR policies and procedures, the following policy development template was developed by state, local, and federal law enforcement and criminal justice partners and is designed to assist justice entity personnel—whether in a law enforcement or homeland security agency, a fusion center, or an intelligence unit—in developing a comprehensive LPR policy.

Justice entities (law enforcement and homeland security agencies, fusion centers, intelligence units, etc.) utilize different types of information (e.g., criminal history, suspicious activity reports [SARs]) and intelligence (e.g., criminal intelligence information) as part of their intelligence or investigative activities. Each type of information and intelligence is governed by laws, regulations, and policies. LPR information, as collected and maintained in an LPR database, is not considered intelligence, criminal history, or SAR information. As such, the laws, regulations, and policies that apply to those types of information and intelligence may not apply to LPR information until such time as it is downloaded and incorporated into an intelligence or investigative case file. The digital image of license plates is maintained in a separate database from all other types of information and does not include additional information that identifies a particular individual. License plate numbers and date/time location collected through an LPR are not, when taken alone, sufficient to identify the individual associated with the vehicle. Even though the LPR information accessed by the justice entity results from an LPR system's automated collection of license plate numbers, it is the investigative and/or analytic process that associates the stored digital license plate image with an identifiable individual.

For these reasons, this policy template was developed to address the collection, receipt, access, use, dissemination, retention, and purging of LPR information that is not yet part of an intelligence or investigative file. Once LPR information is downloaded by entity personnel and incorporated into an intelligence or investigative file, the LPR information is then considered intelligence or investigative information and the laws, regulations, and policies applicable to that type of information or intelligence govern its use.

The provisions suggested in this template are intended to be incorporated into the entity's general operational policies and day-to-day operations and to provide explicit and detailed privacy, civil rights, and civil liberties protection guidance to entity personnel and other authorized source and participating agencies. This policy template was developed based on the core principles articulated in the Fair Information Practice Principles (refer to Appendix B). Each section is a fundamental component of an overall comprehensive LPR policy that includes vital baseline provisions on legal compliance, governance and oversight, acquiring and receiving, use, sharing and dissemination, information quality, redress, security and maintenance, retention and purging, accountability and enforcement, and training concepts.

B. How to Use This Template

This template is designed with policy concepts grouped into related sections. Each section contains pertinent policy provision questions shown in **bold** type. Sample policy language is shown under each question in regular type.

1. Different Entity LPR Roles

There are generally two different ways (or roles) entities come into contact with LPR information:

- Entities that do not collect LPR information but have access to and query an LPR database.
- Entities that actively collect, receive, access (query), disseminate, retain, and purge LPR information.

The policy provisions contained in this template were designed to be customized for either role. Entities that do not collect, receive, and retain LPR information but only access and query an LPR system will find that some provisions may not apply. However, all of the provisions will most likely apply, in some form, to entities that do collect, receive, and retain LPR information. Notations are provided within each applicable provision to allow for customization according to these entity roles.

2. Referencing Other Policies

Frequently, agencies already have established privacy-related policies and practices contained in broader policy documents (e.g., concept of operations, standard operating procedures, user agreements, and employee handbooks). In accordance with template Sections L, Accountability and Enforcement, and L.1, Transparency, agencies are strongly encouraged to make their LPR policies available to the public, even if the other existing policies are not made available publicly. As such, consolidating various existing LPR policy provisions contained in other documents into one LPR policy is highly recommended. Agencies are cautioned, however, against simply providing a cross-reference to other policies in effect. Cross-referencing, without including the applicable policy language, should be done only if those policies are also available to the public; otherwise, agencies should restate (or excerpt) the applicable language within their LPR policy.

3. Template Modifications—Customizing Your Policy

It is important to note that this policy development template is not intended to be used as is, without modification. Each section represents the foundational components of an effective LPR policy but does not cover all concepts that may be particular to your entity, its unique processes and procedures, or the applicable constitutional provisions, laws, ordinances, or regulations within your state. Further, certain concepts or questions may not be applicable. The template represents a starting point for your entity to establish minimum baseline LPR policy protections. Law enforcement entities are encouraged to complete as many of the template questions as are applicable and to enhance sections to include items such as references to applicable statutes, rules, standards, or policies and to provide additional sections for provisions that are not addressed.

While it is important for entities to review each question and associated guidance contained in the policy template section of this document, a sample LPR policy that incorporates all of the sample policy language contained in the template section is provided in Appendix E for ease of customization.

C. Resource List

Resources that may be of interest include:

- *Acceptable Use Policy for the Regional License Plate Reader System*, Automated Regional Justice Information System (ARJIS), www.arjis.org/RegionalPolicies/ARJIS%20LPR%20AUP%20-%20Approved%20-%20Rev150213.pdf.
- Automated License Plate Reader Frequently Asked Questions, International Association of Chiefs of Police (IACP), www.iacp.org/ALPR-FAQs.
- *Automated License Plate Readers: A Primer*, Violence Reduction Network, www.vrnetwork.org/Documents/License%20Plate%20Readers%20primer.pdf.
- *Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement*, IACP, www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf.
- *Best Practices Guide for Improving Automated License Plate Reader Effectiveness Through Uniform License Plate Design and Manufacture*, American Association of Motor Vehicle Administrators (AAMVA), www.aamva.org/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=2911&libID=2897.
- Fair Information Practice Principles, refer to Appendix B.
- *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template*, U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ), April 2010, https://it.ojp.gov/documents/d/Fusion_Center_Privacy_Policy_Development_508compliant.pdf.
- *Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment* (ISE Privacy Guidelines), Office of the Program Manager, Information Sharing Environment (ISE), www.ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf.
- *Initial Privacy Impact Assessment for Automated License Plate Reader Technology*, Northern California Regional Intelligence Center (NCRIC), https://northerncaliforniamostwanted.org/html/NCRIC%20ALPR%20PIA.PDF.
- *IACP Technology Policy Framework,* IACP, January 2014, www.theiacp.org/Portals/0/documents/pdfs/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf.
- *License Plate Readers for Law Enforcement: Opportunities and Obstacles*, RAND Corporation, www.rand.org/pubs/research_reports/RR467.html.
- *License Plate Recognition Technology (LPR) Impact Evaluation and Community Assessment*, George Mason University, http://cebcp.org/wp-content/evidence-based-policing/LPR_FINAL.pdf.
- *License Plate Standard,* American Association of Motor Vehicle Administrators, 2016, www.aamva.org/licenseplatestandard_2016/.
- *Mobile License Plate Reader System Standard for Law Enforcement Working Draft,* NIJ Standard-100x.00, National Institute of Justice, Office of Justice Programs (OJP), DOJ, August 21, 2014, www.justnet.org/pdf/Draft_Mobile_License_Plate_Reader_System_Standard_for_Law_Enforcement.pdf.
- *Privacy, Civil Rights, and Civil Liberties Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component*, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/181/Privacy--Civil-Rights--and-Civil-Liberties-Audit-Guidance-for-the-State--Local--Tribal--and-Territorial-Intelligence-Component.
- *Privacy Impact Assessment for the Acquisition and Use of License Plate Reader Data From a Commercial Service*, U.S. Department of Homeland Security, www.dhs.gov/publication/dhs-ice-pia-039-acquisition-and-use-license-plate-reader-data-commercial-service.
- *Privacy Impact Assessment Report for the Utilization of License Plate Readers*, IACP, www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf.
- *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies*, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.

License Plate Reader (LPR) Policy Development Template for Use in Intelligence and Investigative Activities

A. Purpose Statement

1. What is the purpose of establishing a license plate reader (LPR) policy (i.e., what does the entity hope to accomplish in adopting this policy)? Provide a succinct, comprehensive statement of purpose.

It is the purpose of this policy to provide **[name of entity]** personnel with guidelines and principles for the collection, access, use, dissemination, retention, and purging of LPR information to ensure that the information is used for legitimate law enforcement purposes only and the privacy, civil rights, and civil liberties of individuals are not violated. The Fair Information Practice Principles (FIPPs) form the core of the privacy protection framework for this policy.

This policy assists **[name of entity]** and its personnel in:

- Increasing public safety and improving state, local, tribal, territorial, and national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.
- Promoting governmental legitimacy and accountability.
- Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.
- Minimizing the threat and risk of damage to real or personal property.
- Increasing trust by maximizing transparency.
- Making the most effective use of public resources allocated to public safety entities.

2. What are the entity's authorized uses for LPR information?

The provisions of this policy are provided to support authorized uses of LPR information. Authorized uses may include the following **[include any of the following purposes or others that apply to the entity]**:

- Enhance **[insert state]**'s AMBER/SILVER or other law enforcement alerts and real-time response capability by deploying and networking LPRs 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 LPR 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 violent crime.

- Support **[name of entity]**'s homeland security mission by protecting critical infrastructure from individuals who intend to damage or disrupt the systems and locations that allow for travel and the free flow of commerce.
- 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, driving under the influence initiatives, enforcement details, directed criminal investigations, and other investigations.

B. Policy Applicability and Legal Compliance

1. What information is subject to the LPR policy?

This policy applies to LPR information collected or received, accessed, used, disseminated, retained, and purged by the **[name of entity]**. It is not intended to apply and does not apply to any other types of information accessed, retained, or used by the **[name of entity]**.

2. Who is subject to the LPR policy? Identify who must comply with the LPR policy; for example, entity personnel, participating agencies, and private contractors.

All **[name of entity]** personnel, participating agency personnel and authorized individuals working in direct support of **[name of entity]** personnel (such as interns), personnel providing information technology services to the **[name of entity]**, private contractors, and other authorized users will comply with the **[name of entity]**'s LPR policy. This policy applies to information the **[name of entity]** collects or receives, accesses, uses, disseminates, retains, and purges.

3. How is the entity's LPR policy made available to personnel, participating entities, and individual users (in print, online, etc.), and are acknowledgment of receipt and agreement to comply with this policy required in writing?

The **[name of entity]** will provide a printed or electronic copy of this LPR policy to all:

- **[name of entity]** and non-**[name of entity]** personnel who provide services.
- Participating agencies.
- Individual authorized users.

The **[name of entity]** will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains.

4. This entity requires *personnel and participating information-originating and user agencies* to be in compliance with all applicable constitutional and statutory laws. What are the primary laws with which personnel and participating agencies must comply?

Cite the primary laws with which personnel and participating users must comply that protect privacy, civil rights, and civil liberties in the collection, receipt, access, use, dissemination, retention, and purging of LPR information.

This should include any state statute regarding deployed LPR systems by state or local government. It might also include the U.S. Constitution and state constitutions; open records or sunshine laws; information breach notification laws; other laws, regulations, orders, opinions, or policies impacting or protecting privacy, civil rights, or civil liberties; local ordinances; and relevant federal laws, such as the Driver's Privacy Protection Act and regulations. (For synopses of primary federal laws an entity should consider referencing in the LPR policy, refer to Appendix C, Listing of Federal Laws.)

All **[name of entity]** personnel, participating agency personnel and authorized individuals working in direct support of **[name of entity]** personnel (such as interns), personnel providing information technology services to the **[name of entity]**, private contractors, agencies from which **[name of entity]** information originates, and other authorized users will comply with applicable laws and policies concerning privacy, civil rights, and civil liberties, including, but not limited to **[include a specific reference to any relevant state statutes or other binding state or local policy specific to LPR systems, then provide a list of other applicable state and federal privacy, civil rights, and**

civil liberties laws or include a reference to the section or appendix containing a list of applicable laws]. As part of this process, all individuals working with LPR information will complete the applicable training as directed by **[name of entity]**.

C. Governance and Oversight

1. **Who has primary responsibility for the entity's overall operation, including the entity's justice information systems, information collection and retention procedures, coordination of personnel, and enforcement of this policy? Which individual will ultimately be held accountable for any problems or errors?**

   Primary responsibility for the operation of the **[name of entity]**; its justice information systems, operations, and the coordination of personnel; the receiving, seeking, retention, evaluation, information quality, use, purging, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the **[position/title]** of the **[name of entity]**.

2. **Who is assigned primary responsibility for overseeing and administering the entity's LPR program?**

   The **[name of entity]**'s **[insert title]** will designate an LPR Administrator who will be responsible for the following **[include any of the following responsibilities that apply to the LPR Administrator or other responsibilities]**:

   - Overseeing and administering the LPR program.
   - Ensuring that stored LPR information is automatically purged from the LPR database, unless determined to be of evidentiary value (refer to Section K.1, Information Retention and Purging).
   - Confirming, through random audits, that LPR information is purged in accordance with this policy.
   - Acting as the authorizing official for individual access to LPR information.
   - Ensuring and documenting that all personnel with authorized access to LPR information are trained prior to using the system.
   - Conducting audits to ensure compliance with applicable laws, regulations, standards, and policy.

3. **What is the process for developing, reviewing, and updating the LPR policy?**

   The **[name of entity]** is guided by a **[insert guiding authority, for example, a "designated LPR oversight committee"]** that liaises with the community to ensure that privacy, civil rights, and civil liberties are appropriately protected by this LPR policy and by the **[name of entity]**'s LPR information collection, receipt, access, use, dissemination, retention, and purging processes and procedures.

   Approach 1: The committee will annually review and update the LPR policy in response to changes in law and implementation experience, including the results of audits and inspections, and will solicit input from stakeholders on the development or proposed updates to the LPR policy.

   Approach 2: The committee will annually review and update the LPR policy in response to changes in law and implementation experience, including the results of audits and inspections, and will provide notice to and solicit comment from the public on the development or proposed updates to the LPR policy.

4. **Who is the designated and trained privacy, civil rights, and civil liberties individual or entity who will handle reported errors and violations and oversee the implementation of LPR privacy, civil rights, and civil liberties protections?**

   [Provide the title of the individual or name of the entity. This may be the privacy, civil rights, and civil liberties officer; legal counsel; internal affairs; external entities such as the U.S. Attorney or the Office of Inspector General; or other.]

   The **[insert title of individual or name of entity]** will receive reports regarding alleged errors and violations of the provisions of this LPR policy, will receive and coordinate complaint resolution under the **[name of entity]**'s LPR redress policy, and will ensure that privacy, civil rights, and civil liberties protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The **[insert title of individual but not the name or name of entity]** may be contacted at the following address: **[insert mailing address or e-mail address]**.

5. **Who is responsible for ensuring that enforcement procedures and sanctions for noncompliance with the LPR policy are adequate and enforced?**

   The **[name of entity]**'s **[insert title]** will ensure that enforcement procedures and sanctions outlined in **[insert section number of policy (see Section L.3, Enforcement)]** are adequate and enforced.

D. Definitions

1. **What key words or phrases are regularly used in the LPR policy for which the entity wants to specify particular meanings?**

   This may include terms that are not commonly known or have multiple meanings that may need to be clarified to indicate which one applies to the LPR policy. There may be legal definitions for terms in the statutes governing the operation of justice information or LPR systems. For examples of definitions of key terms commonly used throughout this template, refer to Appendix A, Glossary of Terms and Definitions.

   For examples of primary terms and definitions used in this LPR policy, refer to **[insert section or appendix citation]**.

E. Acquiring and Receiving LPR Information

1. **Describe how the entity acquires LPR information. Use the following provisions that apply to the entity. If neither a. nor b. applies because the entity does not directly collect or indirectly acquire LPR information, skip question 1 and move to question 2. For entities that do directly collect and/or indirectly acquire LPR information, answer the applicable question but also answer question 2, since it is understood that the entity would also query such information.**

   a. **If the entity directly collects LPR information through LPR systems (mobile or stationary), list the authorized purpose upon which that collection is based. Note: State law may restrict collecting LPR information from commercial databases.**

      The **[name of entity]**, through its **[insert name of the entity's LPR program]**, will directly collect and retain LPR information that:

      - Is based on a potential threat to public safety or the enforcement of the criminal law, or
      - Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity, or
      - Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences, or
      - Is directly related to an investigation or mission of the law enforcement entity, and
        - The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
        - The information was collected in a fair and lawful manner (e.g., it does not infringe on the federal or state constitutional rights of any individual, group, or organization).

   b. **Does the entity indirectly acquire LPR information from other law enforcement agencies? If yes, identify the mechanism by which this occurs (e.g., memorandum of understanding [MOU], law, intergovernmental agreement [IGA]).**

      The **[name of entity]** will indirectly acquire LPR information from **[list other law enforcement agency or agencies]** in accordance with **[insert mechanisms, e.g., MOU, law, intergovernmental or interagency agreement]** established between the **[name of entity]** and the law enforcement agency(ies).

2. **For queries of LPR information, list the authorized purpose on which queries are based. Indicate whether the entity queries a law enforcement or commercial database or both. Note: State law may restrict queries to commercial databases.**

   The **[name of entity]** will query **[insert name of law enforcement or commercial database]** LPR information that:

- Is based on a possible threat to public safety or the enforcement of the criminal law, or
- Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity, or
- Is relevant to the 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, or
- Is directly related to an investigation or mission of the law enforcement entity, and
  - The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
  - The information was collected in a fair and lawful manner (e.g., it does not infringe on the federal or state constitutional rights of any individual, group, or organization).

3. Does the entity utilize hot lists (alert lists), and if so, what is the entity's procedure?

Hot-list information is considered confidential information to the extent permitted by law and will be updated **[insert time period(s)]** each day. Officers assigned an LPR unit are responsible for ensuring they are operating with the most current hot list (at minimum) at the beginning of each shift, including information files of stolen and "of interest" vehicles containing all of the current National Crime Information Center (NCIC) information. Department members will query their LPR system to ascertain whether there is a prior read of the license plate that is the subject of the particular alert, bulletin, or alarm. Proactive manual entry of LPR hot lists in the field is permitted for:

- Dispatched reports of crimes—"Be On the Lookouts" (BOLOs) or AMBER, SILVER, or other law enforcement alerts in which a license plate number is part of the broadcast; or
- When directed or authorized for a legitimate law enforcement purpose.

4. Identify what LPR information *may not* be sought, retained, shared, or disclosed by the entity.

This may include federal or state constitutional prohibitions or prohibitions in federal, state, local, or tribal laws.

The **[name of entity]** and any information-originating entities will not seek, submit, or retain LPR information about individuals or organizations based solely on their 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.

5. Identify what information is *contained* in entity-accessed LPR information.

[Name of entity] LPR cameras may be mobile (mounted on vehicles) or stationary (i.e., mounted to a structure). A standard LPR record contains, at a minimum, an optical character recognition (OCR) interpretation of the captured image, a photo of the license plate and a contextual photo of an area surrounding the plate that could range from a few inches to a larger area around the entire vehicle, the geographic coordinates of where the image was captured, the date and time of the recording, and the specific camera/unit that captured the image.

6. Identify what information is *not contained* in entity-accessed LPR information.

[Name of entity]-accessed LPR information contains images of license plates that are available to public view (e.g., vehicles that are on a public road or street or that are on private property but whose license plates[s] are visible from a public road, street, or place to which members of the public have access, such as the parking lot of a shop or other business establishment) and that identify specific vehicles. Retained LPR information does not include specific identification of individuals. Separate video surveillance images of the same location or images from private cameras will not be associated with LPR data unless a specific image is required to investigate or document a violation in accordance with the authorized purposes described in this section.

License plate numbers and date/time location collected through an LPR may not be, when taken alone, sufficient to identify the individual associated with the vehicle. The **[name of entity]** may be able to link the LPR information to an individual through additional use and combination with other information, such as a check of vehicle registration. Thus, even though the LPR information the **[name of entity]** accesses may be the result of an LPR system's automated collection of license plate numbers, it is the investigation process that identifies individuals. Refer to Section H.2 for information on the **[name of entity]**'s LPR validation procedure or to Appendix A, Glossary of Terms and Definitions, for more information on LPR information.

Approach 1: [This approach should be used by entities that withhold LPR information from public release using the privacy exemption under the public records laws.]
The **[name of entity]** protects all LPR information as personally identifiable information (PII) because LPR information may be combined with other information to specify 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). The **[name of entity]** collects, receives, accesses, uses, disseminates, retains, and purges LPR information because it can be linked to an individual to further an authorized mission.

Approach 2:
In the absence of the investigation process, the license plate number and the time and location data attached to it may not identify a specific person. Thus, even though the **[name of entity]**'s LPR systems automate the collection of license plate numbers, it is the investigation process that identifies individuals. Refer to Section H.2 for information on the **[name of entity]**'s LPR validation procedure or to Appendix A, Glossary of Terms and Definitions, for more information on LPR information.

Databases of LPR information do not contain alert lists based on strictly civil matters. In addition, LPR information does not contain audio recordings.

7. Does the LPR policy specifically require a consideration of nondiscriminatory intent in the placement of stationary cameras?

Per the **[name of entity]** policy of nondiscrimination noted in Section E.4, the pattern and frequency of stationary camera placement will be assessed **[note frequency]** to confirm nondiscriminatory placement.

8. Who owns the entity's LPR hardware, software, and LPR information collected?

The hardware and software licenses associated with the **[name of entity]**'s LPR system are the property of **[insert name of owning agency]**, regardless of whether the system has been purchased, leased, or acquired as a service. All deployments of the LPR system are for official use only (FOUO). All information captured, stored, generated, or otherwise produced by an LPR system is the property of the **[insert name of owning agency]**, regardless of where the information is housed or stored.[3]

9. What is the entity's policy regarding the investigative techniques the entity will follow when acquiring LPR information (for example, an intrusion-level statement)?

LPR information collection and investigative techniques used by the **[name of entity]** and by LPR information-originating agencies must be the least intrusive as necessary in the particular circumstances to collect LPR information the **[name of entity]** is authorized to seek or retain.

10. If the entity contracts with commercial LPR databases, does the entity require an assurance that the commercial LPR database company is in legal compliance in its information collection, receipt, access, retention, dissemination, and purging procedures?

The **[name of entity]** will contract only with commercial LPR database companies that provide an assurance that their methods for collecting, receiving, accessing, disseminating, retaining, and purging LPR information comply with applicable local, state, tribal, territorial, and federal laws, statutes, regulations, and policies and that these methods are not based on misleading information collection practices.

11. From what sources (nongovernmental, commercial, or private agencies or institutions or classes of individuals) will the entity not seek, receive, accept, or retain LPR information?

The **[name of entity]** will not directly or indirectly seek, receive, accept, or retain LPR information from:

- An individual who or nongovernmental agency that may receive a fee or benefit for providing the LPR information, except as expressly authorized by law or **[name of entity]** policy, and/or
- An individual who or information provider that is legally prohibited from obtaining or disclosing the LPR information.

[3] Refer to state law regarding ownership and compliance with open record requests regarding LPR information.

F. Use of LPR Information

1. Describe the authorized uses justifying access to or disclosure of LPR information *within the entity or in other governmental agencies*.

Access to or disclosure of LPR information will be provided only ***to individuals within the entity or in other governmental agencies*** who are authorized to have access and only for legitimate law enforcement purposes (e.g., enforcement, reactive investigations) and to IT personnel charged with the responsibility for system administration and maintenance. This means that queries and dissemination of LPR information are permitted only if:

- There is a legal basis requiring these actions, or
- There is reasonable suspicion that an individual or enterprise is involved in criminal conduct or activity, and
  - The LPR information is relevant to that suspected criminal conduct or activity and the requestor has a legitimate need to know.

Examples of legitimate law enforcement purposes to access LPR information may include:

- Enforcement
- Reactive investigations
- Supervisory or security oversight of LPR system and data use

Authorized uses are described in A.2 of this policy. However, the **[name of entity]** accords special consideration to the collection of LPR information relating to First Amendment-protected events and will articulate a legal or justified basis for such collection during the planning assessment and approval process for the particular event, before proceeding with the collection.[4]

2. Which LPR program or LPR information uses are prohibited by the entity?

The **[name of entity]** will prohibit access, use, or dissemination of LPR information for:

- Any purpose that violates the Constitution or laws of the United States, including the protections of the Fourth Amendment.
- Non-law enforcement or personal purposes.
- Discriminatory purposes.
- The purpose of prohibiting, infringing upon, or deterring 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.[5]
- The purpose of prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by and secured by the U.S. Constitution or any other constitutionally protected right or attribute.
- 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, noted in Section E.4.
- Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

3. What types of user actions and permissions are controlled by the entity's LPR access limitations?

<u>Best Practice</u>: Least privilege administration is a recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform. It is suggested that entities specify their method for identifying user actions and permissions as it relates to LPR information within their LPR policies.

In addition, the **[name of entity]** will employ credentialed, role-based access criteria, as appropriate, to control:

- The LPR information to which a particular group or class of users may have access based on the group or class.
- The assignment of roles (e.g., administrator, manager, operator, and user).

[4] For further information about these processes, see *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies* at 4, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.
[5] Ibid. at 6–7 and 11–13.

- The categories of LPR information that a class of users are permitted to use in order to update a hot list, including information being utilized in specific investigations.
- Any administrative or functional access required to maintain, control, administer, audit, or otherwise manage the information or equipment.

G. Sharing and Dissemination of LPR Information

1. Under what conditions will the entity provide external law enforcement agencies with access to the entity's LPR information?

The **[name of entity]** will establish requirements for any external agency requesting access to the **[name of entity]**'s LPR information. These requirements will be documented in an interagency agreement/memorandum of understanding and will include an assurance from the external agency that it complies with the laws and rules governing those individual agencies, including applicable federal and state laws.

2. Under what circumstances will the entity or contracted vendor *not disclose* LPR information?

The **[name of entity]**'s LPR information **will not** be:

- Sold, published, exchanged, or disclosed to commercial or private entities or individuals except as required by applicable law and to the extent authorized by the **[name of entity]**'s agreement with a commercial vendor.
- Disclosed or published without prior notice to the originating entity that such information is subject to disclosure or publication. However, the **[name of entity]** and the originating agency may agree in writing in advance that the **[name of entity]** will disclose LPR information as part of its normal operations, including disclosure to an external auditor of the LPR information.
- Disclosed on a discretionary basis unless the originating agency has provided prior written approval or unless such disclosure is otherwise authorized by the memorandum of understanding or agreement between the **[name of entity]** and the originating agency.
- Disclosed to unauthorized individuals.

[For commercial LPR vendors, the entity should consult its vendor agreement.]

3. State the entity's policy on confirming the existence or nonexistence of LPR information to individuals or agencies that are not authorized to receive the information.

The **[name of entity]** will not confirm the existence or nonexistence of LPR information to any individual or agency that would not be authorized to receive the information unless otherwise required by law.

H. Information Quality Assurance

1. What is the entity's policy for ensuring that the original LPR information is not altered, changed, or modified?

Original LPR 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.

2. For LPR alerts, what procedure must be followed to validate LPR information prior to law enforcement action (for example, prior to law enforcement initiating a traffic stop or investigative act, including analytics)?

Whenever a license plate reader alerts on license plate information, prior to taking any law enforcement action, officers will be required, to the fullest extent possible, to visually verify that the actual vehicle license plate information matches the license plate information used and alerted upon by the LPR system, including both alphanumeric characters of the license plate and the state of issuance; verify the current status of the plate as active through **[insert name of source, such as mobile information terminal [MDT] query, NCIC, etc.]**; and confirm whether the alert pertains to the registrant of the car or the car itself. Receipt of an LPR alert for a stolen or felony vehicle may not rise to the level of reasonable suspicion and is not sufficient probable cause to arrest without confirmation that the alert is still valid and active. If the alert is for another type of transaction, the officer will read the description of the alert and follow the appropriate action or reporting method. If an LPR alert cannot be verified both visually and for validity, then law enforcement should not act on the alert and it should be rejected.

If the officer witnesses a violation of law or other action that establishes reasonable suspicion for a stop, the officer may conduct a stop based on that reasonable suspicion. This provision shall not prevent a law enforcement officer from taking immediate action when a verifiable emergency situation exists for officer safety.

On each resulting alert, the officer is required to enter a disposition indicating the action taken or not taken on the alert.

3. What is the entity's procedure for ensuring proper LPR equipment functionality?

The **[name of entity]** will perform routine maintenance, upgrades, calibration, and refreshes of all LPR equipment and components to ensure proper functionality, including the following:

- At the beginning of a shift, officers will visually inspect the exterior cameras to ensure the lenses are clear and the cameras have not been altered in any way.
- Designated, trained personnel shall check LPR equipment on a regular basis to ensure functionality and proper camera alignment.
- Any equipment that falls outside expected functionality shall be removed from service until deficiencies have been corrected.
- Officers will not attempt to disconnect, modify, or change the LPR equipment or software unless authorized to do so.
- Damage or other malfunctions to the equipment will be reported to the **[insert position/title]**.
- The LPR equipment and components will not be transferred to another vehicle except with the prior, written approval of the LPR Administrator.

4. Does the entity research alleged or suspected errors and deficiencies of LPR information (or requests that the originating agency or vendor investigates)?

The **[name of entity]** will investigate, in a timely manner, alleged errors and deficiencies of LPR information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and deficiencies.

5. How does the entity respond to confirmed errors or deficiencies of LPR information it has originated or received from an originating agency or vendor—for example, camera or system metadata (i.e., camera clock, location, image quality, Global Positioning System [GPS] errors)?

Note: When the original LPR record has been corrected, the [name of entity] should consider how prosecutors (and thus, defense counsel), who may be using the LPR record as evidence in a criminal case, are to be notified of such correction (i.e., written, electronic, other).

The **[name of entity]** will correct, notate, delete, or refrain from using LPR information the **[name of entity]** originated and found to be erroneous or deficient. Originating agencies external to the **[name of entity]** are responsible for reviewing the quality and accuracy of the LPR information provided to the **[name of entity]** and must take reasonable steps to correct or amend the information upon learning that it is inaccurate or deficient. The **[name of entity]** will review the quality of LPR information it has received from an originating agency or vendor and will advise the appropriate point of contact, in writing or electronically, when its LPR information is alleged, suspected, or found to be erroneous or deficient.

6. When the entity has provided erroneous or deficient LPR information to an external agency, what method is used to notify the external agency (written, telephonic, or electronic notification)?

Note: When the original LPR record has been corrected, the [name of entity] should consider how prosecutors (and thus, defense counsel), who may be using the LPR record as evidence in a criminal case, are to be notified of such correction (i.e., written, electronic, other).

The **[name of entity]** will use written or electronic notification to inform recipient agencies **[or, if applicable, use the phrase "inform the consolidated system"]** when LPR information previously provided is erroneous or deficient. In addition, the **[name of entity]** will take reasonable steps to correct or amend the information provided to the external agency in order to ensure accuracy and sufficiency to the extent possible.

I. Redress

I.1 Disclosure

1. **May LPR information be provided *to a member of the public* in response to an information request, and are these circumstances described in the entity's redress policy? For this policy provision, consult with legal counsel to determine under what conditions, if any, LPR information would be disclosed to a member of the public.**

   Notes:
   - **This issue does not apply to circumstances in which an entity chooses to provide sensitive information in accordance with entity policy in response to an emergency situation or provide nonsensitive information to the public.**
   - **For those entities that withhold LPR information from public release using the privacy exemption under public records laws, Approach 1 under E.6 should be selected.**

   LPR information will be disclosed to the public in accordance with **[cite applicable public records laws]**. **[If the state law permits disclosure, revise provision to reflect this.]**

2. **If required by state statute, what is the entity's process for disclosing LPR information to an individual about whom LPR information has been collected or received, and if confirming identity of the requestor is required, is a record kept of all requests?**

   Note: If the state public (open) records act provides procedures for disclosure, corrections, appeals, and handling of complaints when LPR information is not subject to disclosure, these procedures should be summarized in the policy in lieu of using the sample language provided.

   Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity, an individual is entitled to know the existence of and to review the LPR information about him or her that has been collected or received and retained by the **[name of entity]**. If allowed by state law, the individual may obtain a copy of the LPR information for the purpose of challenging the accuracy or completeness of the information (correction). The **[name of entity]**'s response to the request for LPR information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests.

I.2 Corrections

1. **If, in accordance with state statute, the entity is subject to disclosure, what is the entity's procedure for handling individuals' requests for correction involving *LPR information the entity has disclosed and can change because it originated the information*? Is a record kept of requests for corrections?**

   If, in accordance with state law, an individual requests correction of LPR information *originating with the* **[name of entity]** that has been disclosed, the **[name of entity]**'s **[insert title of designee]** will inform the individual of the procedure for requesting corrections, including appeal rights for those requests that are denied in whole or in part. A record will be kept of all requests.

I.3 Appeals

1. **If requests for disclosure or corrections are denied, what is the entity's procedure for appeal?**

   The individual who has requested disclosure or to whom LPR information has been disclosed will be informed of the reason(s) why the **[name of entity]** or originating agency denied the request for disclosure or correction. The individual will also be informed of the procedure for appeal when the **[name of entity]** or originating agency has cited an exemption for the type of information requested or has declined to correct challenged LPR information to the satisfaction of the individual to whom the information relates.

J. Security and Maintenance

1. **What are the entity's physical, procedural, and technical safeguards for ensuring the security of LPR information?**

   Describe how the entity will protect the LPR information from compromise, such as:

   - **Unauthorized access**
   - **Modification**
   - **Theft**
   - **Sabotage (whether internal or external)**
   - **Natural or human-caused disasters**
   - **Intrusions**

   Consider procedures, practices, system protocols, use of software, information technology tools, and physical security measures.

   Best Practice: Reference generally accepted industry or other applicable standard(s) for security with which the entity complies (e.g., National Institute of Standards and Technology guidance).

   The **[name of entity and, if applicable, the name of entity's LPR vendor]** will operate in a secure facility protected from external intrusion and will utilize secure internal and external safeguards against network intrusions. Access to **[name of entity]** LPR information from outside the facility will be allowed only over secure networks.

2. **Is the entity's LPR system in compliance with the manufacturer's recommendations or any current industry standards?**

   All LPR equipment, software, and components will be properly maintained in accordance with the manufacturer's recommendations and/or any published industry standards.

3. **What requirements exist to ensure that the LPR information will be stored in a secure format and a secure environment?**

   The **[name of entity or, if applicable, the name of entity's LPR vendor]** will store LPR information in a manner that ensures that it cannot be added to, modified, accessed, or purged except by personnel authorized to take such actions.

4. **What are the requirements of personnel authorized to have access to entity LPR information?**

   Access to **[name of entity]** LPR 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.

5. **Does the entity prohibit sharing of passwords?**

   Usernames and passwords to LPR information are not transferrable, must not be shared by **[name of entity]** personnel, and must be kept confidential.

6. **Does the entity require specific configurations of strong passwords and require the replacement of manufacturer default passwords for all Web-based system access within a specified time frame?**

   User passwords must meet the following standards **[insert rules, such as no English words and a combination of letters, numbers, and at least two symbols]**. The system administrator will ensure that all manufacturer-generated default passwords are replaced with secure passwords before Web-based interfaces of the system become operational.

7. **Does electronic access to entity LPR information identify the user? Is the identity of the user retained in the audit log?**

   Queries made to the **[name of entity]**'s LPR 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.

8. **Is a log kept of accessed and disseminated entity-owned LPR information, and is an audit trail maintained? Refer to Section L.2, Accountability, for more information on audit logs.**

   The **[name of entity]** will maintain an audit trail of accessed, requested, or disseminated **[name of entity]**-held LPR information. An audit trail will be kept for a minimum of **[specify the retention period for your jurisdiction/entity for this type of request]** of requests for access to LPR information for specific purposes and of what LPR information is disseminated to each individual in response to the request. Audit logs will include:

   - The name and agency of the law enforcement user.
   - The date and time of access.
   - The specific information accessed.
   - The modification or deletion, if any, of the LPR information.
   - The authorized law enforcement or public safety justification for access, including a relevant case number if available. **[Note: The justification should be consistent with Section E.]**

9. **Are risk and vulnerability assessments (if maintained) stored separately from publicly available data?**

   To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

10. **What are the entity's procedures for adhering to information breach notification laws or policies?**

    Best Practice: Provide prompt notification to originating agencies when LPR information they provided to the entity has been the subject of a suspected or confirmed information breach.

    Option 1: State Information Breach Law

    The **[name of entity]** will follow the information breach notification guidance set forth in **[cite to applicable law]**. **Additional Best Practice Sample Language: [To the extent required by the (state) information breach notification law]** The **[name of entity]** will immediately notify the originating agency from which the **[name of entity]** received personal information of a suspected or confirmed breach of such information.

    Option 2: No State Information Breach Law

    A: No State Information Breach Law but the Entity Follows Guidance From the Office of Management and Budget (OMB)
    The **[name of entity]** will follow the information breach notification guidance set forth in OMB Memorandum M-07-16 (May 2007), available at http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf.

    B: Entity Adheres to the Following Policy
    [If there is no applicable state information breach notification law.] The **[name of entity]** will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the individual. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or take any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

K. Information Retention and Purging

1. **What is the entity's policy regarding retention and purging of LPR information? Reference laws, if applicable. If information is stored in multiple repositories (mobile information computer [MDC]/laptops, servers, cameras, etc.), identify each repository and its associated retention period. Agencies vary in their LPR information retention policies based in part on their strategic and tactical objectives in using the technology and the specific laws and regulations of their jurisdictions.**

   All LPR information contained within the **[name of entity]**'s LPR system will be stored for a period not to exceed **[insert a time frame]**. After **[insert time period]**, the information will be automatically purged (i.e., permanently removed from the system).

   [Entities may want to consider different retention periods for LPR information based on the legitimate law enforcement purpose for retaining the record. The following are examples.]

- **When LPR information is used for short-term situational awareness surveillance, the [name of entity] will purge information on nonviolators within [insert time period]. However, with respect to the retention of LPR information relating to First Amendment-protected events (e.g., mass gatherings), the [name of entity] limits the retention of LPR information to [insert time period].**
  Note: In accordance with *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies*,[6] "[a]gencies should limit the retention of information as much as possible to avoid the perception of maintaining files on groups or persons who engage in protected First Amendment activities."
- **For records retained locally on an MDC (and/or back-end servers), the [name of entity] will purge information within [insert time period].**

[The retention decision focuses on the LPR record as a whole. The individual components of the LPR record should not have different retention periods.]

This retention policy applies only to the LPR information contained in the **[name of entity]**'s LPR system itself. Once LPR information is downloaded by **[name of entity]** personnel and incorporated into a criminal intelligence record or an investigative case file, the LPR information is then considered intelligence or investigative information and the laws, regulations, and policies applicable to that type of information or intelligence govern its use.

If the LPR record has become or there is reason to believe that it will become evidence, including evidence that tends to inculpate or exculpate a suspect, in a specific criminal or other law enforcement investigation or action, the following provisions apply:

a. In those circumstances in which an LPR record is identified as having evidentiary value, the LPR **[insert Administrator or other title]** or designee will review the facts of the specific case and determine whether the information should be retained beyond the established retention period. If it is determined that it is reasonable to believe the information has evidentiary value, the LPR **[insert Administrator or other title]** will authorize the transfer of the applicable record from the LPR system server to **[insert appropriate response; for example, "the entity's case management system" or "a form of digital storage media (CD, DVD, etc.) or other portable storage device"]**.
b. Agencies requiring LPR records to be retained by the **[name of entity]** beyond the established retention period may make a formal, written request to the **[name of entity]** to extend retention. Each request must specify the need for extended retention, the circumstances surrounding the request, the requesting agency's case number, and a specific point of contact within the requesting agency. The **[name of entity]** reserves the right to grant or deny agency requests based on the information provided.

The **[name of entity]** retains the right to remove LPR information earlier than the retention period, based on limitations of information storage requirements and subject to applicable statutory disclosure mandates. Early removal, however, will not be used as a means for intentionally interfering with a lawful complaint or a public records request. The retention period may be modified at any time by the **[name of entity]**, subject to applicable legal requirements.

L. Accountability and Enforcement

L.1 Transparency

1. Is the entity's LPR policy available to the public?

The **[name of entity]** will be open with the public in regard to LPR information collection, receipt, access, use, dissemination, retention, and purging practices. The **[name of entity]**'s LPR policy will be made available in printed copy upon request and posted prominently on the **[name of entity]**'s Web site **[or Web page]** at **[insert Web address]**.

2. Does the entity have a point of contact for handling inquiries or complaints?

The **[name of entity]**'s **[Privacy Officer, LPR Administrator, or other position title]** will be responsible for receiving and responding to inquiries and complaints about incorrect information or privacy, civil rights, and civil liberties protections in the LPR information system maintained or accessed by the **[name of entity]**. The **[Privacy Officer, LPR Administrator, or other position title]** may be contacted at **[insert mailing address or e-mail address]**.

[6] Ibid. at 22–23.

L.2 Accountability

1. **What procedures and practices does the entity follow to enable evaluation of user compliance with system requirements, the entity's LPR policy, and applicable law?**

   The **[name of entity]** will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this LPR policy and applicable law. This will include logging access to LPR information and periodic random auditing of these systems, so as not to establish a discernable pattern that may influence users' actions. These audits will be mandated at least **[insert quarterly, semiannually, annually, or other time period]**, and a record of the audits will be maintained by the **[Privacy Officer, LPR Administrator, or title of designee]** of the **[name of entity]**. Audits may be completed by an independent third party or a designated representative of the **[name of entity]**.

   Appropriate elements of this audit process and key audit outcomes will be compiled into a report and may be provided to command staff and oversight entities or governance boards.[7]

   [Entities may also release the results of the audit to the public, pursuant to law or as a matter of discretion. Under these circumstances, consider the following options.]

   Option 1: The **[name of entity]** will provide, at minimum, an overview to the public to enhance transparency with respect to privacy, civil rights, and civil liberties protections built into the **[name of entity]**'s operations.

   Option 2: The **[name of entity]** will also release to the public the full audit, with redactions as necessary to protect the privacy of any individual or group, if appropriate and consistent with jurisdictional requirements.

2. **Does the entity have a mechanism for users or other personnel to report errors and suspected or confirmed violations of LPR policies?**

   The **[name of entity]**'s personnel or other authorized users shall report errors and suspected or confirmed violations of the **[name of entity]**'s LPR policy to the **[name of entity]**'s **[insert title of LPR Administrator]**.

3. **How often does the entity review and update the provisions contained within this LPR policy (for example, annually)?**

   The **[Privacy Officer, LPR Administrator, or other position title]** will review and update the provisions contained in this LPR policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the LPR system; the audit review; and public expectations.

L.3 Enforcement

1. **What is the entity's procedure for enforcement if entity personnel, a participating agency, or an authorized user is suspected of being or has been found to be in noncompliance with the provisions of this policy?**

   If **[name of entity]** personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, receipt, access, use, dissemination, retention, and purging, the **[title of entity Director]** of the **[name of entity]** will:

   - Suspend or discontinue access to information by the **[name of entity]** entity personnel, the participating agency, or the authorized user;
   - Apply appropriate disciplinary or administrative actions or sanctions;
   - If the authorized user is from an agency external to the **[name of entity]**, request that the user's employer initiate disciplinary proceedings to enforce the policy's provisions; and/or
   - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

[7] *Privacy, Civil Rights, and Civil Liberties Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component*, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/181/Privacy--Civil-Rights--and-Civil-Liberties-Audit-Guidance-for-the-State--Local--Tribal--and-Territorial-Intelligence-Component.

2. **What is the entity's policy with regard to the qualifications and number of participating agency personnel authorized to access entity LPR information, and what additional sanctions are available for violations of the entity's LPR policy?**

   The **[name of entity]** reserves the right to establish the qualifications and number of personnel having access to **[name of entity]** LPR information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating this LPR policy.

M. Training

1. **What personnel does the entity require to participate in training programs, before access to entity LPR information is granted, regarding implementation of and adherence to this LPR policy?**

   Before access to **[name of entity]** LPR information is authorized, the **[name of entity]** will require the following individuals to participate in training regarding implementation of and adherence to this LPR policy:

   - All authorized **[name of entity]** personnel.
   - All authorized participating agency personnel.
   - All authorized personnel providing information technology services to the **[name of entity]**.

2. **What is covered by the entity's LPR training program (for example, purpose of the LPR policy, substance and intent of the provisions of the LPR policy, impact of infractions, and possible penalties for violations)?**

   The **[name of entity]**'s LPR policy training program will cover:

   - Purposes of the LPR policy.
   - Substance and intent of the provisions of this LPR policy and any revisions thereto relating to collection, receipt, access, use, dissemination, retention, and purging of the **[name of entity]**'s LPR information and the privacy, civil rights, and civil liberties protections on the use of the technology and the information collected or received.
   - Appropriate procedures relating to license plate image quality and mitigating the risks associated with a possible misread by the LPR system.
   - LPR verification process for law enforcement alerts.
   - Originating and participating agency responsibilities and obligations under applicable federal, state, or local law and policy.
   - How to implement the LPR policy in the day-to-day work of the user, whether a paper or systems user.
   - Mechanisms for reporting violations of **[name of entity]** LPR policy provisions.
   - The nature and possible penalties for LPR policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

(This Page Intentionally Left Blank)

Appendix A—Glossary of Terms and Definitions

The following is a list of primary terms and definitions used throughout this template. These terms are also useful in drafting the definitions section of the entity's LPR policy.

Access—Information access is being able to get to (usually having permission to use) particular information on a computer. Information access is usually specified as edit, enter, modify, or read-only and read/write access. Web access means having a connection to the Internet through an access provider or an online service provider.

Access Control—The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role- or user-based.

Acquisition—The means by which an entity obtains LPR information through the exercise of its authorities.

Agency—A participating agency that accesses, contributes, and/or shares information in the **[name of entity]**'s justice information system.

Aggregation of LPR Data—Refers to information that becomes part of a case file. It is also called "used data," and it shall be compliant with applicable laws and regulations.[8]

Alert—A visual and/or auditory notice that is triggered when the LPR system receives a potential "hit" on a license plate.

Audit Trail—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—What commands were issued to the system? What records and files were accessed or modified?

Audit trails are a fundamental part of computer security and system user accountability and are used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication—The process of validating the credentials of an individual, a computer process, or a device. Authentication requires that the individual, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of usernames and passwords.

Authorization—The process of granting an individual, a computer process, or device access to certain information, services, or functionality. Authorization is derived from the identity of the individual, a computer process, or a device requesting access that is verified through authentication. See Authentication.

[8] Automated License Plate Recognition (ALPR), General Order 17.102, Tempe Police Department, Arizona, 12-13-2003.

Automatic License Plate Reader (ALPR)—ALPR systems comprise high-speed cameras mounted at a fixed location or on a mobile patrol vehicle (see Fixed LPR, Mobile LPR, and Portable LPR definitions) that function to:

- Automatically capture an image of a vehicle's license plate.
- Transform that image into alphanumeric characters using optical character recognition or similar software.
- Compare the plate number acquired to one or more databases of vehicles of interest to law enforcement and other agencies.
- Alert officers when a vehicle of interest has been observed.

The automated capture, use, and comparison of vehicle license plates typically occur within seconds, alerting officers when a wanted plate is observed.[9] A standard LPR record contains, at a minimum, an OCR interpretation of the captured image, a photo of the license plate and a contextual photo of an area surrounding the plate that could range from a few inches to a larger area around the entire vehicle; the geographic coordinates of where the image was captured; the date and time of the recording; and the specific camera/unit that captured the image. Retained LPR information does not include specific identification of individuals.

The following are other names used for this technology:

- Automated license plate recognition (ALPR)
- Automatic license plate recognition (ALPR)
- Automatic number plate recognition (ANPR)
- Automatic vehicle identification (AVI)
- Car plate recognition (CPR)
- License plate recognition (LPR)
- Mobile license plate reader (MLPR)
- Vehicle license plate recognition (VLPR)

Be On the Lookout (BOLO)—Refers to an indication by a law enforcement agency that there is an articulable and specific law enforcement reason to identify or locate a particular vehicle or, in the case of a post-scan BOLO, that there is an articulable and specific reason to ascertain the past location(s) of a particular vehicle.

BOLO List—Also known as a hot list, a compilation of one or more license plates or partial license plates of a vehicle or vehicles for which a BOLO situation exists that is programmed into an LPR so that the device will alert if it captures the image of a license plate that matches a license plate included on the BOLO list. The term also includes a compilation of one or more license plates or partial license plates that is compared against stored license plate information that had previously been scanned and collected by an LPR, including scanned license plate information that is stored in a separate information storage device or system. See Hot List.

Civil Liberties—According to the U.S. Department of Justice's Global Justice Information Sharing Initiative, the term "civil liberties" refers to fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals.

Civil Rights—The term "civil rights" refers to those rights and privileges of citizenship and equal protection that the state is constitutionally bound to guarantee all citizens regardless of race, ethnicity, religion, gender, national origin, religion, sexual orientation, gender identity, or other characteristics unrelated to the worth of the individual. Protection of civil rights imposes an affirmative obligation upon government to promote equal protection under the law. Generally, the term "civil rights" involves positive (or affirmative) government action to protect against infringement, while the term "civil liberties" involves restrictions on government.[10]

Collect—For purposes of this document, "gather" and "collect" mean the same thing.

Confidentiality—Refers to the obligations of individuals and entities to appropriately use information and data under their control once they have been disclosed to them and in accordance with applicable data security laws and policies. See Privacy.

Credentials—Information that includes identification and proof of identification that are used to gain access to local and network resources. Examples of credentials are usernames, passwords, smart cards, and certificates.

Criminal Activity—A behavior, an action, or an omission that is punishable by criminal law.[11]

Criminal Case Support—Those administrative or analytic activities that provide relevant information to law enforcement personnel regarding the investigation of specific criminal activities or trends or specific subject(s) of criminal investigations.[12]

Data Breach—The unintentional release of secure information to an untrusted environment. Your response to a data breach may be addressed in state law or agency policy. This may include incidents such as:

- Theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted.

[9] Automated License Plate Recognition, "About ALPR" Web page, International Association of Chiefs of Police, http://www.iacp.org/ALPR-About.

[10] Civil Rights and Civil Liberties Protections Guidance (September 2008). The definition of "civil rights" is a modified version of the definition contained in the *National Criminal Intelligence Sharing Plan* (NCISP), at pp. 5–6.

[11] *License Plate Reader—Standard Operating Procedure*, Appendix—Definitions, Maryland Coordination and Analysis Center, www.mcac.maryland.gov/resources/LPR/LPR-SOP.html.

[12] Ibid.

- Posting such information on the Internet.
- Unauthorized employee access to certain information.
- Moving such information to a computer otherwise accessible from the Internet without proper information security precautions.
- Intentional or unintentional transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail.
- Transfer of such information to the information systems of a possibly hostile entity or environment where it may be exposed to more intensive decryption techniques.

Direct LPR Collection—The entity is the owner of the LPR equipment that captures LPR information.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, an entity, or an organization outside the entity that collected it.

Dissemination—See Disclosure.

Electronically Maintained—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, compact disc optical media, or cloud technologies.

Electronically Transmitted—Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, or transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voicemail.

Entity—The **[name of entity],** which is the subject and owner of the LPR policy.

Fair Information Practice Principles—The Fair Information Practice Principles (FIPPs) are a set of internationally recognized principles that inform information privacy policies both within government and the private sector. Although specific articulations of the FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into information privacy laws, policies, and governance documents around the world. They provide a straightforward description of underlying privacy and information exchange principles and a simple framework for the legal use that needs to be done regarding the impact of an LPR system on individual privacy. Some of the individual principles, such as Principle 7, may not apply in all instances of an integrated justice system.

The eight principles are:

1. Collection Limitation/Data Minimization
2. Data Quality/Integrity (See definition.)
3. Purpose Specification
4. Use Limitation
5. Security Safeguards (See definition.)
6. Openness/Transparency
7. Individual Participation
8. Accountability/Audit

See Appendix B for one description of how the U.S. Department of Homeland Security applies these principles.

Firewall—A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

Fixed LPR—LPR cameras that are permanently affixed to a structure, such as a pole, a traffic barrier, or a bridge.

Hit—A read matched to a plate which has previously been registered on an agency's "hot list" of vehicle plates related to stolen vehicles, wanted vehicles, or other factors supporting investigation or which has been manually registered by a user for further investigation.

Hot List—A file that contains the license plate numbers of stolen vehicles; stolen license plates; AMBER, SILVER, or other law enforcement alerts; lists of license plate numbers known to be associated with specific individuals, such as wanted individuals or missing individuals (e.g., wanted for homicide, rape, robbery, child abduction); or terrorist watch lists. The Motor Vehicle Administration also provides suspended or revoked registrations. A hot list is routinely updated but does not rely on real-time communications with state or federal information sources. LPR hot lists are compiled to serve agency-specified needs. Manual entry may be available, allowing additions for specific license plates. The hot list is essential to LPR systems, as it is required in order to notify law enforcement that a vehicle on the list is near an LPR camera.[13] See Be On the Lookout.

Identification—A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that uniquely differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a collection of data, such as a given and family name, date of birth, and address. An organization's identification process consists of the acquisition of the relevant identifying information.

Information—Inert symbols, signs, descriptions, or measures; elements of information. Includes any information about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement entities can be categorized into four general areas: general data, including

[13] Ibid.

investigative information; tips and leads data; suspicious activity reports; and criminal intelligence information.

Information Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, receipt, use, dissemination, retention, purging, and protection of information.

Information Quality (IQ)—Refers to various aspects of the information; the accuracy and validity of the actual values of the data, information structure, and database/information repository design. Traditionally, the basic elements of IQ have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, IQ is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy. This concept is also addressed as one of the Fair Information Practice Principles, Data Quality/Integrity. See Appendix B for a full set of the FIPPs.

Information Sharing Environment (ISE)—In accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, the Information Sharing Environment (ISE) is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of state, local, tribal, and territorial (SLTT) agencies; federal agencies; and the private sector to facilitate terrorism-related information sharing, access, and collaboration.

Invasion of Privacy—Intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See also Right to Privacy.

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform.

Legitimate Law Enforcement Purpose—The investigation, detection of a crime, or a violation of the law and/or the operation of terrorist or missing or endangered individual searches or alerts.[14]

Linkable Information—Information about or related to an individual for whom there is a possibility of logical association with other information about that individual.[15]

Linked Information—Information about or related to an individual that is logically associated with other information about that individual.[16]

Logs—A necessary part of an adequate security system because they are needed to ensure that information is properly tracked and that only authorized individuals are getting access to the data. See also Audit Trail.

LPR—Refer to Automatic License Plate Reader (ALPR).

LPR Information[17]—The images and the metadata associated with them are the primary forms of information collected by an LPR system. Information files typically contain the following information:

- Black-and-white plate image
- Contextual color image
- Electronically readable format of plate
- Alphanumeric characters of license plate numbers
- Location and GPS coordinates
- Time and date of image capture
- Camera identification

LPR System—A set of equipment used to capture license plate images and associated data. The equipment may include the following:

- One or more LPR cameras
- Processor for converting the images to text
- Optical Character Recognition (OCR) engine optimized for reading license plates
- GPS receiver
- Brackets or mounting hardware
- Connect cables

See also Automatic License Plate Reader, Fixed LPR, Mobile LPR, or Portable LPR.

Maintenance of Information—Applies to all forms of information storage. This includes electronic systems (for example, databases) and nonelectronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves that organization's purpose.

Mobile LPR—Intended for use in a moving motor vehicle (i.e., camera is moving) and typically mounted semipermanently to a marked patrol vehicle. A mobile LPR typically includes one to four cameras and the configuration is set at the discretion of the contributing agency based on driving patterns and street configurations.

Need to Know—As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counterterrorism activity or other authorized government duty, such as to further an investigation or meet another law enforcement requirement.

[14] Ibid.
[15] Automated License Plate Recognition (ALPR), General Order 17.102, Tempe Police Department, Arizona, 12-13-2003.
[16] Ibid.
[17] Automated License Plate Recognition (ALPR), General Order 17.102, Tempe Police Department, Arizona, 12-13-2003.

Nonencounter Alert—Refers to an immediate alert in which the officer operating the LPR is instructed to notify the agency that put out the alert without initiating an investigative detention of the subject vehicle or otherwise revealing to the occupant(s) of that vehicle that its location has been detected or that it is the subject of law enforcement attention.

Nonrelevant Information—Information regarding a vehicle's location—particularly when collected over an extended period of time—may be misused to infer additional information about an individual that is not relevant to police purposes and potentially sensitive for the individual. Such inferences may include but are not limited to nonrelevant personal relationships, marital fidelity, religious observance, and political activities such as attending rallies or vote canvassing. By precisely and proportionally limiting access to LPR information, the risks of such misuse can be reduced and the likelihood of inferring protected/nonrelevant character attributions can be minimized. In addition, by ensuring that information lawfully collected but determined to be nonrelevant is purged upon classification as nonrelevant, entities further mitigate the privacy risks.

Participating Entity—A public safety or law enforcement agency that owns and/or operates LPR cameras, contributes information to the LPR system, and is authorized to access or receive entity LPR information.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, a directory, or a printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personal Information—Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in criminal activity, including terrorism. See also Personally Identifiable Information (PII).

Personally Identifiable Information (PII)—One or more pieces of information that, when considered alone, in the context of how the information is presented or gathered, or when combined with other information, are sufficient to specify a unique individual. The pieces of information can be, but are not limited to:

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).
- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, social media user name, driver's license number, financial account or credit card number and associated PIN number, Integrated Automated Fingerprint Identification System [IAFIS] identifier, or booking or detention system number).
- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Portable LPR—LPR cameras that are transportable and can be moved and deployed in a variety of venues as needed, such as a traffic barrel or speed radar sign.

Privacy—Refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy—A printed, published statement that articulates the policy position of an organization on how it handles the personal information that it collects or receives and accesses or uses in the normal course of business. The policy should include information relating to the processes of information collection, receipt, access, use, dissemination, retention, and purging. It is likely to be informed by the Fair Information Practice Principles (FIPPs). The purpose of the privacy policy is to articulate that the entity will adhere to those legal requirements and entity policy determinations that enable collection, receipt, access, use, dissemination, retention, and purging of information to occur in a manner that protects personal privacy interests.

Public—Public includes:

- Any individual and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the entity's information.
- Media organizations.
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit and without distinction as to the nature or intent of those requesting information from the entity or participating entity.

Public does not include:

- Any employees of the entity or participating entity.
- People or entities, private or governmental, who assist the entity in the operation of the justice information system.
- Public entities whose authority to access information collected or received and retained by the entity is specified in law.

Public Access—Relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

Purge—A term that is commonly used to describe methods that permanently erase and remove data from a storage space. There are many different strategies and techniques for data purging, which is often contrasted with data deletion.

Read—Digital images of license plates and associated metadata (e.g., date, time, and geographic coordinates associated with the vehicle image capture) that are captured by the LPR system.

Record—Any item, collection, or grouping of information that includes PII and is collected, received, accessed, used, disseminated, retained, and purged by or for the collecting entity or organization.

Redress—Laws, policies, and procedures that address public entity responsibilities with regard to access/disclosure and correction of information and the handling of complaints from individuals regarding *protected information* about them which is under the entity's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

Protected information includes personal information about individuals that is subject to information privacy or other legal protections by law. Protection may also be extended to organizations by center policy or state, local, tribal, or territorial law.

Retention—Refer to Storage.

Right to Know—Based on having legal authority or responsibility or pursuant to an authorized agreement, an entity or an organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, counterterrorism activity, or other authorized government duty.

Right to Privacy—The right to be left alone, in the absence of some reasonable public interest in collecting, accessing, retaining, and disseminating information about an individual's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the individual or entity violating an individual's privacy.

Role-Based Access—A type of access authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.

Scan—Refers to the process by which an LPR automatically focuses on, photographs, and converts to digital text the license plate of a vehicle that comes within range of the LPR.

Security—Refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of information for the legitimate user set, as well as promoting failure resistance in the electronic systems overall. Security safeguarding of information is a Fair Information Practice Principle. See Appendix B.

Source Entity—Refers to the entity or organizational entity that originates LPR information.

Storage—In a computer, storage is the place where information is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

Storage is frequently used to mean the devices and information connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This is probably the most common meaning in the IT industry.

In a more formal usage, storage has been divided into (1) primary storage, which holds information in memory (sometimes called random access memory, or RAM) and other "built-in" devices, such as the processor's L1 cache, and (2) secondary storage, which holds information on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more information than primary storage.

User—An entity employee or an individual representing a participating entity who is authorized to access or receive and use an entity's information and intelligence databases and resources for lawful purposes.

Appendix B—Fair Information Practice Principles (FIPPs)

The Fair Information Practice Principles (FIPPs) are a set of internationally recognized principles that inform information privacy policies within both government and the private sector.

Although specific articulations of the FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into data privacy laws, policies, and governance documents around the world. For example, the FIPPs are:

- At the core of the Privacy Act of 1974, which applies these principles to U.S. federal agencies.[18]
- Influential internationally, especially as articulated by the Organisation for Economic Co-operation and Development.
- Mirrored in many states' laws and in fusion centers' privacy policies.
- Used by numerous foreign countries and international organizations.

The following formulation of the FIPPs is used and implemented for the Information Sharing Environment (ISE) by the U.S. Department of Homeland Security (DHS).[19] For a definition of the Information Sharing Environment, refer to Appendix A, Glossary of Terms and Definitions.

1. **Purpose Specification—**Agencies should specifically articulate the authority that permits the collection of personally identifiable information (PII). The purpose(s) for which PII is collected should be specified at the time of data collection. Subsequent use of this data should be limited to the original purpose for which the PII was collected (or other purposes *compatible* with the original collection purpose).

   Implementing the Purpose Specification Principle—Agencies are bound by specific constitutional and statutory authorities that circumscribe their ability to collect PII. The following are examples of ways agencies may implement this principle:

   - Ensure that a valid lawful purpose exists and is documented for all collection of PII.
   - Include the source and authority for the data so that access restrictions can be applied.
   - Upon receipt of data containing PII from third parties, if possible, identify the purpose for which it was collected initially and limit agency use to only those uses compatible with the original purpose supporting collection.
   - Ensure that metadata or other tags are associated with the data as it is shared.
   - Institute a two-individual review and approval process to consider any Privacy Act or other legal or policy limitation before permitting use or sharing of data for purposes other than that for which it was collected.

2. **Data Quality/Integrity—**PII collected should be relevant to the purposes identified for its use and should be accurate, complete, and up to date.

[18] 5 U.S.C. § 552a.
[19] 6 U.S.C.§ 142.

Implementing the Data Quality/Integrity Principle—One important way to minimize potential downstream privacy and civil liberties concerns is to ensure that any information collected, stored, and disseminated is accurate. This includes ensuring that the information provides sufficient context for any PII. Possible approaches include:

- Properly labeling PII.
- Determining a policy for safeguarding PII if there are "mixed" databases (i.e., those databases with personal information on U.S. individuals and others, regardless of nationality).
- Instituting a source verification procedure to ensure reporting is based only on authorized data.
- Reconciling and updating PII whenever new relevant information is collected.
- Developing a protocol for ensuring data corrections are passed to those entities with which information has been shared.
- Creating a documented process for identifying and addressing situations in which data has been erroneously received, is inaccurate or has been expunged.

3. **Collection Limitation/Data Minimization—**PII should be collected only if the data is directly relevant and necessary to accomplish the specified purpose. PII should be obtained by lawful and fair means and retained only as long as is necessary to fulfill the specified purpose.

   Implementing the Collection Limitation/Data Minimization Principle—Collection limitation may be implemented by:

   - Designing a data storage system to pull data for review and then, if appropriate, automatically purging data after the specified retention period has been reached.
   - Limiting data field elements to only those that are relevant.
   - Ensuring that all distributed reports and products contain only that personal information that is relevant and necessary (nothing extraneous or superfluous).
   - Ensuring that all shared information with PII meets required thresholds for sharing, such as reasonable suspicion.

4. **Use Limitation—**PII should not be disclosed, made available, or otherwise used for purposes other than those specified except (a) with the consent of the individual or (b) by the authority of law.

   Implementing the Use Limitation Principle—Sharing information should be tempered by adherence to key principles, such as "authorized access." Use limitation may be implemented by:

   - Limiting users of data to those with credential-based access.
   - Requiring that justifications be entered and logs maintained for all queries with sensitive PII and that an internal review process of those logs takes place at specified intervals.
   - Requiring senior analysts to review all reports that use PII before dissemination to ensure (a) that PII is relevant and necessary and (b) that the recipient is authorized to receive the information in the performance of an authorized activity.
   - Prior to sharing information, verify that partners have a lawful purpose for requesting information.
   - Creating multiple use-based distribution lists and restricting distribution to those authorized to receive the information.

5. **Security/Safeguards—**Agencies should institute reasonable security safeguards to protect PII against loss, unauthorized access, destruction, misuse, modification, or disclosure.

   Implementing the Security/Safeguards Principle—This principle can be implemented by:

   - Maintaining up-to-date technology for network security.
   - Ensuring that access to data systems requires that users meet certain training and/or vetting standards and that such access is documented and auditable.
   - Ensuring that physical security measures are in place, such as requiring an identification card, credentials, and/or passcode for data access; disabling computers' USB ports; and implementing firewalls to prevent access to commercial e-mail or messaging services.
   - Implementing a protocol with technical and manual safeguards to ensure the accuracy and completeness of data system purges when records are deleted at the end of their retention period.
   - Ensuring that data system purge protocols include complete record deletion on all backup systems.
   - Transitioning older repositories into more modern systems to improve access controls.
   - Masking data so that it is viewable only to authorized users.

- Maintaining an audit log to record when information is accessed and by whom for review by senior staff at specified intervals.
- Requiring authorized users to sign nondisclosure agreements.

6. **Accountability/Audit—**Agency personnel and contractors are accountable for complying with measures implementing the FIPPs, for providing training to all employees and contractors who use PII, and for auditing the actual use and storage of PII.

   Implementing the Accountability/Audit Principle—Strong policies must not only be in place but also be effectively implemented. Accountability can be demonstrated by:

   - Ensuring that upon entry for duty, all staff take an oath to adhere to the privacy and civil liberties protections articulated in the center's or host agency's mission, core values statements, other key documents, and/or the U.S. Constitution.
   - Conducting effective orientation and periodic refresher training, including privacy, civil rights, and civil liberties protections, for all individuals handling PII.
   - Tailoring training to specific job functions, database access, or data source/storage requirements.
   - Conducting regular audits of all systems in which records are kept to ensure compliance with privacy, civil rights, and civil liberties policies and all legal requirements.
   - Following a privacy incident, establishing a handling procedure for any data breaches or policy violations.
   - Denying database access to individuals until they have completed mandatory systems access training (including training for handling of PII), show a mission need for access, and have any necessary clearances.
   - Developing targeted and consistent corrective actions whenever noncompliance is found.

7. **Openness/Transparency—**To the extent feasible, agencies should be open about developments, practices, and policies with respect to the collection, use, dissemination, and maintenance of PII. Agencies should publish information about policies in this area, including the privacy, civil rights, and civil liberties policy, and contact information for data corrections and complaints.

   Implementing the Openness/Transparency Principle—Agencies can implement the Openness/Transparency principle by:

   - Providing reports to an internal or external oversight body concerned with privacy, civil rights, and civil liberties issues, including privacy, civil rights, and civil liberties audit results.
   - Publishing the privacy, civil rights, and civil liberties policy and redress procedures.
   - Meeting with community groups through initiatives or other opportunities to explain the agency's mission and privacy, civil rights, and civil liberties protections.
   - Responding in the fullest way possible to freedom of information and/or sunshine requests and fully explaining any denial of information requests from the public.
   - Conducting and publishing Privacy Impact Assessments (PIAs) in advance of implementing any new technologies that affect PII thereby demonstrating that privacy, civil rights, and civil liberties issues have been considered and addressed.

8. **Individual Participation—**To the extent practicable, involve the individual in the process of using PII and seek individual consent for the collection, use, dissemination, and maintenance of PII. Agencies should also provide mechanisms for appropriate access, correction, and redress regarding the agency's use of PII.

   Implementing the Individual Participation Principle—To the extent appropriate, agencies can implement the Individual Participation principle by:

   - Collecting information directly from the individual, to the extent possible and practical.
   - Providing the individual with the ability to find out whether a project maintains a record relating to him or her and, if not (i.e., access and/or correction is denied), then providing the individual with notice as to why the denial was made and how to challenge such a denial.
   - Putting in place a mechanism by which an individual is able to prevent information about him or her that was obtained for one purpose from being used for other purposes without his or her knowledge.

(This Page Intentionally Left Blank)

Appendix C—Listing of Federal Laws

The U.S. Constitution is known as the primary authority that applies to federal as well as state, local, tribal, and territorial (SLTT) entities. State constitutions cannot provide a lower level of privacy and other civil liberties protection than that established by the U.S. Constitution, but states can broaden constitutional rights guaranteed by their own constitutions.

Civil liberties protections are primarily founded in the Bill of Rights. They include the basic freedoms, such as free speech, assembly, and religion; freedom from unreasonable search and seizure; due process; etc. Statutory civil rights protections in the U.S. Constitution may, in addition, directly govern state action. These include the Civil Rights Act of 1964, as amended; the Rehabilitation Act of 1973; the Equal Educational Opportunities Act of 1974; the Americans with Disabilities Act; the Fair Housing Act; the Voting Rights Act of 1965; and the Civil Rights of Institutionalized Individuals Act.

While SLTT entities may not be generally bound directly by most statutory federal privacy and other civil liberties protection laws in the LPR information collection sharing context, compliance may be required **indirectly** by funding conditions (e.g., Title VI of the Civil Rights Act of 1964), operation of the Commerce Clause of the U.S. Constitution, or a binding agreement between a federal agency and an SLTT entity (e.g., a memorandum of agreement or a memorandum of understanding). When relevant or possibly relevant, entities/agencies are advised to list laws, regulations, and policies within their LPR policy, noting those that may potentially affect the sharing of information.

The development of an LPR policy is primarily designed for entity personnel and authorized users to ensure that they are aware of the legal and privacy framework within which they and the entity must operate. If the applicability and requirements of various laws, regulations, or sharing agreements are not spelled out or referenced in an entity's LPR policy, staff and user accountability is greatly diminished, mistakes are made, privacy violations occur, and the public's (and other agencies') confidence in the ability of the entity to protect LPR information is compromised. When staff members know the rules through sound policy and procedure communicated through ongoing training activity, LPR information sharing is enhanced.

"At the time of this writing there are no federal laws that explicitly govern or limit the use of ALPR technology or taking photographs of things that are plainly visible from public spaces by law enforcement agencies."[20] Many jurisdictions are actively developing or considering legislation that will authorize, limit, and/or restrict the use of ALPR systems and the information they generate. Some examples of specific legislative proposals and legislation that have passed include:

- **Arkansas:** Act 849 of 2015, To Allow the Arkansas Highway Police Division of the Arkansas State Highway and Transportation Department to Utilize the Automatic License Plate Reader System, and Act 1491 of 2013, To Regulate the Use of Automatic License Plate Reader Systems
- **California:** Senate Bill 34 of 2015, Automatic License Plate Recognition Systems: Use of Data
- **Colorado:** House Bill 14-1152, Concerning Passive Surveillance Records of Governmental Entities
- **Florida:** Senate Bill 226
- **Illinois:** SB 1351 - Automated License Plate Recognition System Information Act (2/18/15)
- **Tennessee:** Senate Bill 1664

[20] Automated License Plate Reader Frequently Asked Questions Web page, IACP, www.iacp.org/ALPR-FAQs.

- **Utah:** Senate Bill 196, License Plate Reader Amendments (2013); Senate Bill 222 (LPR amendment; and Senate Bill 51 (LPR Amendment)
- **Maine:** Title 29 Section 2117
- **Maryland:** Senate Bill 699, Automatic License Plate Readers and Captured Plate Data – Authorized Uses
- **Minnesota:** Senate Bill 86, A bill for an act relating to data practices; classifying data related to automated license plate readers and requiring a governing policy; requiring a log of use; requiring data to be destroyed in certain circumstances; and requiring a report
- **North Carolina:** Senate Bill 182, An Act to Regulate the Use of Automatic License Plate Reader Systems
- **Vermont:** Senate Bill 18, An Act Relating to Privacy Protection[21]

The following are synopses of primary federal laws that an entity should review and, where appropriate, consider citing in an LPR policy to protect the LPR record and any personally identifiable information later associated with the LPR record. As LPR information may be incorporated as one piece of information into a larger case file, the following federal laws may be applicable. The list is arranged in alphabetical order by popular name.

1. **Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721—Prohibition on Release and Use of Certain Personal Information from State Motor Vehicle Records—**Collected LPR information contains no personally identifiable information that may be used to connect a license plate detection to an individual. It is only with permissible purpose that law enforcement may make this connect (using other systems) and this access is governed by the Driver's Privacy Protection Act of 1994.

2. **E-Government Act of 2002, Public Law 107–347, 208, 116 Stat. 2899 (2002**)**—**This act requires federal agencies to perform Privacy Impact Assessments (PIAs) for new information technologies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing information technology that manages information in identifiable form. A PIA is an evaluation of how information in identifiable form is collected, stored, protected, shared, and managed. The purpose of a PIA is to demonstrate that system owners and developers have incorporated privacy protections throughout the entire life cycle of a system. The act requires an agency to make PIAs publicly available, except when an agency in its discretion determines publication of the PIA would raise security concerns or reveal classified (i.e., national security) information or sensitive (e.g., potentially damaging to a nation interest, law enforcement effort, or competitive business interest contained in the assessment) information. Although this act does not apply to SLTT partners, this tool is useful for identifying and mitigating privacy risks and for notifying the public what PII the SLTT agency is collecting, why PII is being collected, and how the PII will be collected, used, accessed, shared, safeguarded, and stored.

3. **Federal Civil Rights Laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983—**This is a federal statute that allows an individual to sue public officials in federal court for violations of the individual's civil rights. Civil rights include the Fourth Amendment's prohibitions against unreasonable search and seizure, violations of privacy rights, and violations of the right to freedom of religion, free speech, and free association. It serves as a deterrent to unlawful collection, use, or sharing of information rather than providing specific authority or a prohibition to the collection, use, or sharing of information.

4. **Federal Driver's Privacy Protection Act (DPPA), 18 USC § 2721-2725**—Restricts access and prohibits the release of personal information from state motor vehicle records to ensure the privacy of citizens.

5. **Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301**—This chapter contains the laws governing disposal of records made or received by a federal agency in the normal course of business. It discusses purging procedures and notices, if required, and the role of the federal archivist. The law applies only to federal agencies, but there may be similar state or local laws applicable to state and local agencies.

6. **Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552—**The federal FOIA, enacted in 1966, provides access to federal agency records or information. It does not, however, allow access to state or local government records. Nearly all states have their own public access statutes that provide access to state- and local-agency records. The interaction of federal and state FOIA laws can create complex issues. Federal statutes, in essence, provide a baseline of legal protections for individuals. While state legislatures may pass laws to supplement these federal guidelines, state laws that interfere with or are contrary to a federal law are preempted. By virtue of the Supremacy Clause of the U.S. Constitution (Article VI, Clause 2), federal law may restrict access to records otherwise available pursuant to a state's FOIA by requiring that certain

[21] For more information on state legislation that was introduced/considered regarding LPRs, refer to the National Conference of State Legislatures, ALPR State Legislation page, www.ncsl.org/research/telecommunications-and-information-technology/2014-state-legislation-related-to-automated-license-plate-recognition-information.aspx; for further information, see ALPR Policy and Privacy, IACP, www.iacp.org/ALPR-Policy.

information be kept confidential. Thus, federal confidentiality requirements may supersede a state FOIA statute mandating public disclosure of a record, but only when there is a specific federal statute (other than the federal FOIA) that mandates the records be kept confidential. In short, records may be available under one FOIA statute but not pursuant to another.

7. **Indian Civil Rights Act of 1968, 25 U.S.C. § 1301 et seq., United States Code, Title 25, Chapter 15, Subchapter I—**This act contains definitions of relevant terms and extends certain constitutional rights to Indian tribes exercising powers of self-government.

8. **National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490—**In each state, an authorized criminal justice agency of the state shall report child abuse crime information to or index child abuse crime information in the national criminal history background check system. A criminal justice agency can satisfy the requirement by reporting or indexing all felony and serious misdemeanor arrests and dispositions. The U.S. Attorney General (AG) is required to publish an annual statistical summary of child abuse crimes. The act requires that 80 percent of final dispositions be entered in the state databases by December 1998, with steps being taken toward 100 percent entry.

   A 1994 amendment required that the AG—in consultation with federal, state, and local officials, including officials responsible for criminal history record systems, and representatives of public and private care organizations and health, legal, and social welfare organizations—shall develop guidelines for the adoption of appropriate safeguards by care providers and by the state for protecting children, the elderly, and individuals with disabilities from abuse.

9. **NIST Special Publication 800-53 (Appendix J) *Security and Privacy Controls for Federal Information Systems and Organizations*—**Federal agencies are required to ensure that privacy protections are incorporated into information security planning. To that end, SP 800-53 Rev. 4 features eight families of privacy controls that are based on the FIPPs. The proliferation of social media, Smart Grid, mobile, and cloud computing as well as the transition from structured to unstructured information and metadata environments have added significant complexities and challenges for federal organizations in safeguarding privacy. These challenges extend well beyond the traditional information technology security view of protecting privacy, which focused primarily on ensuring confidentiality. The use of these standardized privacy controls will provide a more disciplined and structured approach for satisfying federal privacy requirements and demonstrating compliance with those requirements. Like their federal partners, SLTT agencies may use the privacy controls when evaluating their systems, processes, and programs.

10. **Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a—**The Privacy Act establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals, which is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by using the name of the individual or some identifier assigned to that individual. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one of 12 statutory exceptions. The act also provides individuals with a means by which to seek access to and amendment of their records and sets agency record-keeping requirements. In addition, the Privacy Act requires that agencies give the public notice of their systems of records by publication in the *Federal Register*.

11. **Protection of Sensitive Agency Information, Office of Management and Budget Memorandum M-06-16 (June 2006)—**This memorandum provides a security checklist from the National Institute of Standards and Technology (NIST) to protect remote information removed from or accessed from outside an agency's physical location specific to personally identifiable information (PII). The NIST checklist requires that agencies verify PII in need of protection, confirm the adequacy of organization policy surrounding PII protection, and implement any necessary protections for PII transported or stored off-site or accessed remotely. In addition to the NIST checklist, the memorandum recommends implementing information encryption on all mobile devices, allowing remote access only with two-factor authentication, using timeout functions on devices, and logging all computer-readable information extracts from databases with sensitive information, while verifying that each extract has either been erased within 90 days or its use is still required.

12. **Safeguarding Against and Responding to the Breach of Personally Identifiable Information, OMB Memorandum M-07-16 (May 2007)—**This memorandum applies to federal agency-held information and information systems, requiring development and implementation of a breach notification policy applicable to personally identifiable information in the possession of the agency. Development of a breach notification policy includes a review of existing privacy and security requirements, development of requirements for incident reporting and handling, and procedures for internal and external notification. SLTT agencies that are not subject to an existing breach notification law or policy may use the federal requirements as a template for developing their own breach notification policy.

13. **U.S. Constitution, First, Fourth, Fifth, Sixth, and Fourteenth Amendments—**The Bill of Rights establishes minimum standards for the protection of the

civil rights and civil liberties of Americans. The First Amendment protects religious freedom, speech, the press, the right to peaceably assemble, and the right to petition the government for a redress of grievances. The Fourth Amendment protects the people from unreasonable searches and seizures and requires that warrants be issued only upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the individual or things to be seized. The Sixth Amendment establishes the right of an accused individual to a speedy and public trial by an impartial jury, to be informed of the nature and cause of the charges, to confront witnesses, to have compulsory process to obtain witnesses, and to have the assistance of legal counsel. The Fourteenth Amendment addresses citizenship rights and equal protection of the laws. Although the equal protection clause applies explicitly only to state governments, equal protection requirements apply to the federal government through the Fifth Amendment Due Process Clause.

14. **Section 210401 of the Violent Crime Control and Law Enforcement Act of 1994, 42 U.S.C. § 14141—** This is a federal statute that provides that it shall be unlawful for any governmental authority or its agent to engage in a pattern or practice of conduct by law enforcement officers that violates the Constitution or laws of the United States. It authorizes the Attorney General to bring civil actions to obtain injunctive or declaratory relief to eliminate the unlawful or unconstitutional pattern or practice.

Appendix D—Cases and Authorities

A. Fourth Amendment Privacy Law

Katz v. United States, 389 U.S. 347 (1967), provides the foundation for most federal court privacy rulings and doctrines. *Katz* moved away from previous Supreme Court privacy jurisprudence in holding that the Fourth Amendment protects people and not places and departed from the previous "trespass" doctrine of Fourth Amendment protection. Fourth Amendment considerations no longer required a physical invasion or trespass. This case began with federal charges placed against defendant Charles Katz for violating a federal law prohibiting the use of interstate communications for placing wagers and bets. Law enforcement had witnessed Katz making calls from a public telephone booth and thereafter placed microphones on the exterior of the telephone booth in order to eavesdrop on his private conversations. The Court found that no physical invasion of the phone booth had occurred but stated that this was not necessary to constitute a search for purposes of the Fourth Amendment. Rather, *Katz* established a two-prong test to determine whether the Fourth Amendment is implicated and a search has occurred. If an individual, like Katz, has manifested an intent to make the information private *and* society accepts that expectation of privacy as reasonable, then that privacy expectation cannot be violated without following Fourth Amendment warrant requirements. In this case, the Court stated that the defendant assumed his conversations were private because he sought to exclude others when he entered the enclosed telephone booth. The Court concluded, "The government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied when using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."

Smith v. Maryland, 442 U.S. 735 (1979), forms the basis of the "third-party exposure" doctrine of electronic privacy law. In Smith, the government used pen register technology to record the numbers dialed out from a certain phone number. This information was used to convict the defendant of robbery. The defendant challenged the use of the pen register as an illegal search under the Fourth Amendment. The *Smith* Court explained that "[c]onsistently with *Katz*, this Court uniformly has held that the application of the Fourth Amendment depends on whether the individual invoking its protection can claim a 'justifiable,' a 'reason,' or a 'legitimate expectation of privacy' that has been invaded by government action. This inquiry . . . normally embraces two discrete questions. The first is whether the individual, by his conduct, has exhibited an actual (subjective) expectation of privacy' . . . . The second question is whether the individual's subjective expectation of privacy is 'one that society is prepared to recognize as reasonable.'" Id. at 740. The Court held that the defendant did not have a reasonable expectation of privacy in the phone record information because the information was automatically turned over to a third party, the phone company. Even if the defendant had an expectation of privacy in the numbers dialed, it was not one society recognized as reasonable—therefore, there was no Fourth Amendment violation.

United States v. Knotts, 460 U.S. 276, 280 (1983) (citing *Katz v. United States*, 389 U.S. 347 (1967)), examined whether a defendant had a reasonable expectation of privacy when travelling on public streets and highways. In *Knotts*, law enforcement placed a beeper in a drum of chloroform in order to track the movements of the vehicle holding the container. The information derived from the radio beeper led the police to a remote cabin where a warrantless search revealed a drug lab. The Court relied heavily on a quote from ***Smith v. Maryland***, 442 U.S. 735 (1979), elaborating on the principles articulated in *Katz*. See *Knotts*, 460 U.S. at 480-081, quoting *Smith*, 442 U.S. at 740. ("Consistently with

Katz, this Court uniformly has held that the application of the Fourth Amendment depends on whether the individual invoking its protection can claim a 'justifiable,' a 'reason,' or a 'legitimate expectation of privacy' that has been invaded by government action. This inquiry . . . normally embraces two discrete questions. The first is whether the individual, by his conduct, has exhibited an actual (subjective) expectation of privacy' . . . . The second question is whether the individual's subjective expectation of privacy is 'one that society is prepared to recognize as reasonable.'") Applying this test, *Knotts* determined that tracking the vehicle did not constitute a search because an "individual travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another" and noted that such movements could have been observed by the naked eye.

United States v. Karo, 468 U.S. 705, 708 (1984), is a case in which a U.S. Drug Enforcement Administration (DEA) agent learned that defendants had ordered 50 gallons of ether from a government informant, who explained that the ether was to be used to extract cocaine from clothing that had been imported into the United States. The government obtained a court order authorizing the installation and monitoring of a beeper in a can of ether, which allowed the government to track the defendant's location. The ether was moved in succession to multiple locations. The information from the beeper led the government to a private residence. Using information derived from the beeper, the government obtained and executed a search warrant, which led to the discovery and seizure of cocaine. Relying on *Katz* and *Knotts*, the Court held that locational information received while the radio transmitter was on public roads was constitutional because Defendant Karo did not have a reasonable expectation of privacy while driving on the roads. However, monitoring the beeper while it was in a private residence, a location that is not opened to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of that residence. On this latter holding, the *Karo* Court distinguished *Knotts* on the grounds that the beeper was not monitored while it was located in a private residence.

Kyllo v. United States, 533 U.S. 27 (2001), establishes the Supreme Court rule on advanced technology use in searches. In *Kyllo*, the police suspected the defendant of growing marijuana inside his residence. They utilized thermal imaging equipment to "peer through" the walls of the home and determined the defendant was growing marijuana. The court of appeals upheld the search on the basis that the defendant did not make any effort to conceal the heat emanating from his home and therefore did not have a reasonable expectation of privacy under the Fourth Amendment. The Supreme Court reversed, holding that the thermal imaging infiltrated the home and did constitute a search under the Fourth Amendment. The Supreme Court ruled that it was a search in violation of the Fourth Amendment because the thermal imaging gained information, through technology not generally used by the public that could not have otherwise been gained without physical intrusion of the home, a constitutionally protected area without a warrant.

United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), is a case that addressed the constitutionality of the warrantless use of a GPS device by examining the privacy risks associated with prolonged collection of location information. The *Maynard* Court stated that those employing GPS trackers "can deduce whether the individual being tracked is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about an individual, but all such facts." Id. at 562. Under this theory, discrete bits of data, when compiled and viewed together over time, may create a mosaic of the individual's habits, relationships, and beliefs. The Court thus extended the privacy protections articulated in *Katz* to situations in which extensive tracking of public movements would reveal a composite profile, when compiled, about an individual and thus held that the police action was a search because it defeated the defendant's reasonable expectation of privacy. Accord *United States v. Jones,* 132 S. Ct. *945, 954 (2012)* (Sotomayor, concurring); but see Orin S. Kerr, The Mosaic Theory of the Fourth Amendment, 111 MICH L. REV. 311 (2012)).

United States v. Jones, 132 S. Ct. 945 (2012), is a case involving law enforcement's placement of a Global Positioning System (GPS) device on a subject's car and use of the device to monitor the vehicle's movement on public streets for a four-week period (which extended beyond the period of time and place authorized by a search warrant). Citing *Katz*, the government argued that no search occurred because Jones had no reasonable expectation of privacy in the area of the vehicle accessed by the government and in the locations of the vehicle on the public roads since they were visible to the public. The Supreme Court Justices rejected this argument and unanimously agreed that use of the GPS device constituted a search within the meaning of the Fourth Amendment. The majority explained that a physical intrusion into a constitutionally protected area, coupled with an attempt to obtain information, can constitute a violation of the Fourth Amendment based upon a theory of common law trespass. The majority explained that "the use of longer-term GPS monitoring in investigations of most offenses impinges on expectations of privacy." Additionally, in a separate opinion, Justice Sotomayor explained that it may be time to rethink all police use of tracking technology, not just long-term GPS, reasoning that "GPS monitoring generates a precise, comprehensive record of an individual's public movement that reflects a wealth of detail about her familial, political, religious, and sexual associations . . . .The government can store such records and efficiently mine them for years to come."

The unanimous decision in ***Riley v. California***, 134 S. Ct. 2473 (2014), demonstrated the United States Supreme Court's willingness to extend Fourth Amendment protections to mitigate the privacy risks associated with the use of new technologies. The Court contrasted a search of information on the cell phone with a search of physical items, saying that such analogy is akin to "saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from Point A to Point B but little else justified lumping them together." The Court also emphasized that "the fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone-seized incident to an arrest is accordingly simple—get a warrant."

B. ALPR and Privacy Law

New Jersey v. Donis, 157 N.J. 44 (N.J. 1998). The New Jersey Supreme Court has held that police are permitted to randomly (i.e., without probable cause) check a license plate number against the state DMV database of any vehicle they encounter while on patrol, accessing only public information such as registration, license status, and whether the car has been reported as stolen. If the inquiry discloses a basis for further police action, then the officer may access the personal information of the registered owner. This case establishes a nondisclosure rule to protect the legitimate privacy interests of motorists.

United States of America v. Curtis Ellison, 462 F.3d 557 (6th Cir. 2006), *cert. denied*, 552 U.S. 947 (2007). The United States Court of Appeals for the Sixth Circuit held that random license plate checks are not an unconstitutional invasion of privacy and that "so long as the officer had a right to be in a position to observe the defendant's license plate, any such observation and corresponding use of the information on that plate does not violate the Fourth Amendment." In reaching this holding, the *Ellison* Court relied on a central tenet of Fourth Amendment jurisprudence established in ***Katz v. United States***, 389 U.S. 347 (1967)—"that the Fourth Amendment protects only what an individual seeks to keep private," and recognized that "objects falling in the plain view of an officer who has a right to be in the position to have that view are subject to seizure . . . ." Id. at 561 (*internal citation omitted*). The court analogized license plates to an automobile's Vehicle Identification Number (VIN), "located inside the passenger compartment, but visible from outside the car," and noted that a VIN does not receive Fourth Amendment protection. Like a VIN, the purpose of a license plate number is "to provide identifying information to law enforcement officials and others." Quoting and applying the reasoning in ***New York v. Class***, 475 U.S. 106 (1986), regarding VINs, the *Ellison* Court determined that "because of the important role played by the [license plate] in the pervasive governmental regulation of the automobile and the efforts by the Federal Government to ensure that the [license plate] is placed in plain view," a motorist can have no reasonable expectation of privacy in the information contained on it. ***Ellison***, 462 F.3d at 561, quoting ***Class***, 475 U.S. at 114.

The ***Ellison*** Court also rejected the notion that the entry of the license plate number into a law enforcement database creates a privacy interest in the nonprivate information retrieved in response to a query, reasoning that "[t]he obvious purpose of maintaining law enforcement databases is to make information, such as the existence of outstanding warrants, readily available to officers carrying out legitimate law enforcement duties." In fact, the computer investigation in this case was "far less invasive than other government actions that fall" outside the purview of the Fourth Amendment. ***Ellison***, 462 F.3d at 562, citing ***Oliver v. United States,*** 466 U.S. 170, 177, 104 S.Ct. 1735, 80 L.Ed.2d 214 (1984) (entering private property with "No Trespassing" signs to observe marijuana plants in an "open field" not visible from outside the property); ***Dow Chemical Co. v. United States,*** 476 U.S. 227, 239, 106 S.Ct. 1819, 90 L.Ed.2d 226 (1986) (photographing an industrial complex with a precision aerial mapping camera); ***California v. Ciraolo,*** 476 U.S. 207, 213-14, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986) (using aerial surveillance in public airspace to observe the curtilage of a private residence); and ***Smith v. Maryland,*** 442 U.S. 735, 745-46, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979) (placing a pen register on a phone line to record the numbers dialed from a private residence). This case is distinguishable from a situation in which the police use a technology not available to the public to discover evidence that could not otherwise be obtained without "intrusion into a constitutionally-protected area." ***Kyllo v. United States,*** 533 U.S. 27, 34-35, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (holding that the use of thermal-imaging technology to detect heat inside a private home violates the Fourth Amendment). The ALPR technology used in this case does not enable law enforcement to access any previously unobtainable information; it simply allows them to access information more quickly. Given that the information was obtained without intruding upon a constitutionally protected area, the *Ellison* Court held that there was no "search" for purposes of the Fourth Amendment. ***Ellison***, 462 F.3d at 563, citing ***United States v. Matthews,*** 615 F.2d 1279, 1285 (10th Cir. 1980); ***United States v. Walraven,*** 892 F.2d 972, 974 (10th Cir.1989); ***Olabisiomotosho v. City of Houston,*** 185 F.3d 521, 529 (5th Cir.1999); ***United States v. Sparks,*** 37 Fed. Appx. 826, 829 (8th Cir.2002); ***Hallstein v. City of Hermosa Beach,*** 87 Fed.Appx. 17, 19 (9th Cir.2003); ***United States v. $14,000.00 in U.S. Currency,*** No. 98-4380, 2000 WL 222587, at *3 (6th Cir. Feb. 14, 2000) (finding no Fourth Amendment violation in a computer check of a license plate); ***United States v. Batten,*** 73 Fed. Appx. 831, 832 (6th Cir. 2003; *see also* **WAYNE R. LAFAVE**, 1 Search & Seizure § 2.5(b) (4th ed. 2004).

The decision in ***Ellison*** has been extensively cited for the proposition that a "motorist has no reasonable expectation of privacy in information contained on his license plate under the Fourth Amendment." See, e.g., ***Yamba v. Harper***, 2010 U.S. Dist. LEXIS 21288 (W.D. Pa. Mar. 9, 2010); ***Cincerella v. Egg Harbor Twp. Police Dep't***, 2009 U.S. Dist. LEXIS 22950 (D.N.J. Mar. 23, 2009); ***United States v. Crooks***, 2008 U.S. Dist. LEXIS 35189 (D. Del. Apr. 29, 2008); ***United States v. Lurry***, 2010 U.S. Dist. LEXIS 118494 (W.D. Tenn. Nov. 8, 2010); ***Brooks. v. Pickett***, 2008 U.S. Dist. LEXIS 27796 (E.D. Mich. Apr. 7, 2008); ***United States v. Miranda-Sotolongo***, 2016 U.S. App. LEXIS 11816 (7th Cir. Ill. June 28, 2016); ***United States v. Diaz-Castaneda***, 494 F.3d 1146, 2007 U.S. App. LEXIS 17005 (9th Cir. Or. 2007); ***Martinez v. State***, 2010 Del. Super. LEXIS 195 (Del. Super. Ct. Apr. 29, 2010); ***Milam v. Commonwealth***, 2013 Ky. App. Unpub. LEXIS 992 (Ky. Ct. App. Aug. 30, 2013); ***Gentry v. Commonwealth***, 2012 Ky. App. Unpub. LEXIS 1040 (Ky. Ct. App. Oct. 12, 2012); ***State v. Sloan***, 193 N.J. 423, 939 A.2d 796, 2008 N.J. LEXIS 22 (2008).

C. Implications of Automation

U.S. Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989). The U.S. Supreme Court acknowledged the distinction between public records that might result from a diligent search of courthouse files, county clerks' offices, and local police stations throughout the United States and a computerized summary maintained in a single clearinghouse of information. The Court held that the electronic compilation of otherwise publicly available but hard to obtain information changed the privacy interest implicated by disclosure of that compilation. The process of automation overcame the "practical obscurity" associated with manually collecting and linking the public records associated with a particular individual into a comprehensive criminal history record. (Note: The Society of American Archivists defines *practical obscurity* as "the principle that private information in public records is effectively protected from disclosure as a result of practical barriers to access." *Practical Obscurity*, SOC'Y AM. ARCHIVISTS, available at http://www2.archivists.org/glossary/terms/p/practical-obscurity.)

D. Civil Rights and Civil Liberties

Green v. City & County of San Francisco, 751 F.3d 1039 (9th Cir. 2014), arose out of a vehicular stop performed by an officer after the agency's automatic license plate reader mistakenly identified the car that a woman was driving as a stolen vehicle. She was stopped, held at gunpoint by multiple officers, handcuffed, forced to her knees, and detained for up to 20 minutes and released once the officers ran her plate and discovered the ALPR mistake and that her vehicle was not stolen. The Ninth Circuit Court of Appeals reversed the district court's grant of summary judgment in favor of the defendant, reinstating the plaintiff's claims of a Fourth Amendment violation and instructing that such claims raised questions of fact for a jury. See also **Department of Homeland Security, *Privacy Impact Assessment for the Acquisition and Use of LPR Information from a Commercial Service,*** at 7 (2013), citing ***Green***, 751 F.3d 1039, and identifying misidentification of a vehicle and its occupants as a privacy risk. ("A license plate read sent to ICE may be incomplete or inaccurate because the license plate is bent, dirty, or damaged, or because the individual reading the numbers makes an error. This can result in the misidentification of a vehicle and its occupants.")

$14,000 in U.S. Currency, 211 F.3d 1270, 2000 U.S. App. Lexis 2429 (6th Cir. 2000). The claimant filed a motion to suppress the $14,000 subject to the forfeiture proceedings, arguing constitutional violations. With regard to the claimant's Fourteenth Amendment claim, the court acknowledged that "it would violate the Equal Protection Clause of the Fourteenth Amendment for an officer to run computer checks in an 'intentionally racially discriminatory manner," citing ***United States v. Travis,*** 62 F.3d 170, 174 (6th Cir. 1995), cert. denied in 516 U.S. 1060, 116 S. Ct. 738 (1996) ("consensual searches may violate the Equal Protection Clause when they are initiated solely based on racial considerations"). The claimant's Equal Protection claim was rejected by the court because the claimant failed to meet his burden of proof of establishing that the officer decided to conduct the computer check of his license plate based solely upon the race of the claimant and the other occupant in the car.

E. Guidance and Policy

International Association of the Chiefs of Police, *Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement*, at 32 (2012), advising that agencies using ALPR technology should address a range of privacy issues, including "[w]hat ALPR information is collected, how the information is collected, how long the information are retained, who can access the information and for what purposes, and what kind of analytic tools and methodologies are available to query and use ALPR information."

U.S. Department of Homeland Security, *Privacy Impact Assessment for the Acquisition and Use of LPR Information from a Commercial Service,* at 7 (2013), available at https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-lpr-march2015.pdf. As explained in this PIA, U.S. Immigration and Customs Enforcement (ICE) uses information obtained from LPRs as one investigatory tool in support of its criminal investigations and civil immigration enforcement actions (i.e., in furtherance of open cases, investigations, or ongoing enforcement actions and only when

necessary based on a law enforcement need). This PIA assesses the potential impact of the use of information obtained from LPRs on the civil liberties of the public and explains the measures to be put in place, in addition to the framework of privacy and civil liberties protections, to mitigate such concerns.

U.S. Department of Justice, *Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity* (December 2014), at https://www.justice.gov/sites/default/files/ag/pages/attachments/2014/12/08/use-of-race-policy.pdf, articulating the standards that should guide use by federal law enforcement officers of race, ethnicity, gender, national origin, religion, sexual orientation, and gender identity in law enforcement or intelligence activities.

(This Page Intentionally Left Blank)

Appendix E—Sample LPR Policy

The following is a sample LPR Policy that contains all of the sample policy language shown after each question in the template section of this document. However, while drafting an LPR policy using this language, it is important that the policy author still review each question and its associated guidance in the template section in tandem with customizing this language. To assist with this task, the policy language contained here mirrors the same structure and policy categories as those reflected in the template so that the template questions may be followed, item by item, while customizing this language. Further, it is critical that entities drafting a policy not cut and paste this language and use it as is, without making modifications. There are many areas that prompt for insertions and entity customization. These are shown **bolded and in brackets [ ]**. Also, this policy may not cover all concepts that are unique to your entity's specific LPR program or there may be provisions that are not applicable that should be deleted. Throughout the sample policy, law enforcement entities are encouraged to enhance language with references to applicable statutes, rules, standards, or policies.

Finally, since this guidance resource promotes transparency with the public, entities should ensure their policy is written not only for the understandability of entity personnel but also for the understandability of members of the public. While some of the provisions here may reflect concepts and processes long understood and integrated into the daily work of law enforcement such that an entity may not feel they are necessary in the policy, they are still provided here for the purposes of informing the general public, who may not be aware of such processes, and articulating the entity's position and procedures for protecting privacy, civil rights, and civil liberties throughout the entity LPR program.

A. Purpose Statement

1. It is the purpose of this policy to provide **[name of entity]** personnel with guidelines and principles for the collection, access, use, dissemination, retention, and purging of LPR information to ensure that the information is used for legitimate law enforcement purposes only and that privacy, civil rights, and civil liberties of individuals are not violated. The Fair Information Practice Principles (FIPPs) form the core of the privacy framework for this policy.

This policy assists **[name of entity]** and its personnel in:

- Increasing public safety and improving state, local, tribal, territorial, and national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.
- Promoting governmental legitimacy and accountability.
- Minimizing the potential risks to individual privacy, civil rights, civil liberties and other legally protected interests.
- Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.
- Minimizing the threat and risk of damage to real or personal property.
- Increasing trust by maximizing transparency.
- Making the most effective use of public resources allocated to public safety entities.

2. The provisions of this policy are provided to support authorized uses of LPR information. Authorized uses may include the following **[include any of the following purposes or others that apply to the entity]**:

- Enhance **[insert state]**'s AMBER/SILVER or other law enforcement alerts and real-time response capability by deploying and networking LPRs 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 LPR 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 violent crime.
- Support **[name of entity]**'s homeland security mission by protecting critical infrastructure from individuals who intend to damage or disrupt the systems and locations that allow for travel and the free flow of commerce.
- 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, driving under the influence initiatives, enforcement details, directed criminal investigations, and other investigations.

B. Policy Applicability and Legal Compliance

1. This policy applies to LPR information collected or received, accessed, used, disseminated, retained, and purged by the **[name of entity]**. It is not intended to apply and does not apply to any other types of information accessed, retained, or used by the **[name of entity]**.

2. All **[name of entity]** personnel, participating agency personnel and authorized individuals working in direct support of **[name of entity]** personnel (such as interns), personnel providing information technology services to the **[name of entity]**, private contractors, and other authorized users will comply with the **[name of entity]**'s LPR policy. This policy applies to information the **[name of entity]** collects or receives, accesses, uses, disseminates, retains, and purges.

3. The **[name of entity]** will provide a printed or electronic copy of this LPR policy to all:

- **[name of entity]** and non-**[name of entity]** personnel who provide services.
- Participating agencies.
- Individual authorized users.

The **[name of entity]** will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains.

4. All **[name of entity]** personnel, participating agency personnel and authorized individuals working in direct support of **[name of entity]** personnel (such as interns), personnel providing information technology services to the **[name of entity]**, private contractors, agencies from which **[name of entity]** information originates, and other authorized users will comply with applicable laws and policies concerning privacy, civil rights, and civil liberties, including, but not limited to **[include a specific reference to any relevant state statutes or other binding state or local policy specific to LPR systems, then provide a list of other applicable state and federal privacy, civil rights, and civil liberties laws or include a reference to the section or appendix containing a list of applicable law]**. As part of this process, all individuals working with LPR information will complete the applicable training as directed by **[name of entity]**.

C. Governance and Oversight

1. Primary responsibility for the operation of the **[name of entity]**; its justice information systems, operations, and the coordination of personnel; the receiving, seeking, retention, evaluation, information quality, use, purging, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the **[position/title]** of the **[name of entity]**.

2. The **[name of entity]**'s **[insert title]** will designate an LPR Administrator who will be responsible for the following **[include any of the following responsibilities that apply to the LPR Administrator or other responsibilities]**:

- Overseeing and administering the LPR program.
- Ensuring that stored LPR information is automatically purged from the LPR database, unless determined to be of evidentiary value (refer to Section K.1, Information Retention and Purging).

- Confirming, through random audits, that LPR information is purged in accordance with this policy.
- Acting as the authorizing official for individual access to the LPR information.
- Ensuring and documenting that all personnel with authorized access to LPR information are trained prior to using the system.
- Conducting audits to ensure compliance with applicable laws, regulations, standards, and policy.

3. The **[name of entity]** is guided by a **[insert guiding authority, for example, a "designated LPR oversight committee"]** that liaises with the community to ensure that privacy, civil rights, and civil liberties are appropriately protected by this LPR policy and by the **[name of entity]**'s LPR information collection, receipt, access, use, dissemination, retention, and purging processes and procedures.

Approach 1: The committee will annually review and update the LPR policy in response to changes in law and implementation experience, including the results of audits and inspections and will solicit input from stakeholders on the development or proposed updates to the LPR policy.

Approach 2: The committee will annually review and update the LPR policy in response to changes in law and implementation experience, including the results of audits and inspections and provide notice to and solicit comment from the public on the development or proposed updates to the LPR policy.

4. The **[insert title of individual or name of entity]** will receive reports regarding alleged errors and violations of the provisions of this LPR policy, will receive and coordinate complaint resolution under the **[name of entity]**'s LPR redress policy, and will ensure that privacy, civil rights, and civil liberties protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The **[insert title of individual but not the name or name of entity]** may be contacted at the following address: **[insert mailing address or e-mail address]**.

5. The **[name of entity]**'s **[insert title]** will ensure that enforcement procedures and sanctions outlined in **[insert section number of policy (see Section L.3, Enforcement)]** are adequate and enforced.

D. Definitions

1. For examples of primary terms and definitions used in this LPR policy, refer to **[insert section or appendix citation]**.

E. Acquiring and Receiving LPR Information

1. The **[name of entity]**, through its **[insert name of the entity's LPR program]**, will directly collect and retain LPR information that:

- Is based on a potential threat to public safety or the enforcement of the criminal law, or
- Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity, or
- Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences, or
- Is directly related to an investigation or mission of the law enforcement entity, and
  - The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
  - The information was collected in a fair and lawful manner (e.g., it does not infringe on the federal or state constitutional rights of any individual, group, or organization).

The **[name of entity]** will indirectly acquire LPR information from **[list other law enforcement agency or agencies]** in accordance with **[insert mechanisms, e.g., MOU, law, intergovernmental or interagency agreement]** established between the **[name of entity]** and the law enforcement agency(ies).

2. The **[name of entity]** will query **[insert name of law enforcement or commercial database]** LPR information that:

- Is based on a possible threat to public safety or the enforcement of the criminal law, or
- Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any

individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity, or

- Is relevant to the 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, or
- Is directly related to an investigation or mission of the law enforcement entity, and
  - The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
  - The information was collected in a fair and lawful manner.

3. Hot-list information is considered confidential information to the extent permitted by law and will be updated **[insert time period(s)]** each day. Officers assigned an LPR unit are responsible for ensuring they are operating with the most current hot list (at minimum) at the beginning of each shift, including information files of stolen and "of interest" vehicles containing all of the current National Crime Information Center (NCIC) information. Department members will query their LPR system to ascertain whether there is a prior read of the license plate that is the subject of the particular alert, bulletin, or alarm. Proactive manual entry of LPR hot lists in the field is permitted for:

- Dispatched reports of crimes—"Be On the Lookouts" (BOLOs) or AMBER, SILVER, or other law enforcement alerts in which a license plate number is part of the broadcast; or
- When directed or authorized for a legitimate law enforcement purpose.

4. The **[name of entity]** and any information-originating entities will not seek, submit, or retain LPR information about individuals or organizations based solely on their 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.

5. **[Name of entity]** LPR cameras may be mobile (mounted on vehicles) or stationary (mounted to a structure). A standard LPR record contains, at a minimum, an optical character recognition (OCR) interpretation of the captured image, a photo of the license plate and a contextual photo of an area surrounding the plate that could range from a few inches to a larger area around the entire vehicle, the geographic coordinates of where the image was captured, the date and time of the recording, and the specific camera/unit that captured the image.

6. **[Name of entity]**-accessed LPR information contains images of license plates that are available to public view (e.g., vehicles that are on a public road or street or that are on private property but whose license plates[s] are visible from a public road, street, or place to which members of the public have access, such as the parking lot of a shop or other business establishment) and that identify specific vehicles. Retained LPR information does not include specific identification of individuals. Separate video surveillance images of the same location or images from private cameras will not be associated with LPR data unless a specific image is required to investigate or document a violation in accordance with the authorized purposes described in this section.

License plate numbers and date/time location collected through an LPR may not be, when taken alone, sufficient to identify the individual associated with the vehicle. The **[name of entity]** may be able to link the LPR information to an individual through additional use and combination with other information, such as a check of vehicle registration. Thus, even though the LPR information the **[name of entity]** accesses may be the result of an LPR system's automated collection of license plate numbers, it is the investigation process that identifies individuals. Refer to Section H.2 for information on the **[name of entity]**'s LPR validation procedure or to Appendix A, Glossary of Terms and Definitions, for more information on LPR information.

Approach 1:
The **[name of entity]** protects all LPR information as personally identifiable information (PII) because LPR information may be combined with other information to specify 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). The **[name of entity]** collects, receives, accesses, uses, disseminates, retains, and purges LPR information because it can be linked to an individual to further an authorized mission. **[For those entities that withhold LPR information from public release using the privacy exemption under public records laws, Approach 1 should be selected.]**

Approach 2:
In the absence of the investigation process, the license plate number and the time and location data attached to it may not identify a specific person. Thus, even though the **[name of entity]**'s LPR systems automate the collection of license plate numbers, it is the investigation process that identifies individuals. Refer to Section H.2 for information on the **[name of entity]**'s LPR validation procedure or to Appendix A, Glossary of Terms and Definitions, for more information on LPR information.

Databases of LPR information do not contain alert lists based on strictly civil matters. In addition, LPR information does not contain audio recordings.

7. Per the **[name of entity]** policy of nondiscrimination noted in Section E.4, the pattern and frequency of stationary camera placement will be assessed **[note frequency]** to confirm nondiscriminatory placement.

8. The hardware and software licenses associated with the **[name of entity]**'s LPR system are the property of **[insert name of owning agency]**, regardless of whether the system has been purchased, leased, or acquired as a service. All deployments of the LPR system are for official use only (FOUO). All information captured, stored, generated, or otherwise produced by an LPR system is the property of the **[insert name of owning agency]**, regardless of where the information is housed or stored.[1]

9. LPR information collection and investigative techniques used by the **[name of entity]** and by LPR information-originating agencies must be the least intrusive as necessary in the particular circumstances to collect LPR information the **[name of entity]** is authorized to seek or retain.

10. The **[name of entity]** will contract only with commercial LPR database companies that provide an assurance that their methods for collecting, receiving, accessing, disseminating, retaining, and purging LPR information comply with applicable local, state, tribal, territorial, and federal laws, statutes, regulations, and policies and that these methods are not based on misleading information collection practices.

11. The **[name of entity]** will not directly or indirectly seek, receive, accept, or retain LPR information from:

- An individual who or nongovernmental agency that may receive a fee or benefit for providing the LPR information, except as expressly authorized by law or **[name of entity]** policy, and/or
- An individual who or information provider that is legally prohibited from obtaining or disclosing the LPR information.

F. Use of LPR Information

1. Access to or disclosure of LPR information will be provided only to individuals within the **[name of entity]** or in other governmental agencies who are authorized to have access and only for legitimate law enforcement purposes (e.g., enforcement, reactive investigations) and to IT personnel charged with the responsibility for system administration and maintenance. This means that queries and dissemination of LPR information are permitted only if:

- There is a legal basis requiring these actions, or
- There is reasonable suspicion that an individual or enterprise is involved in criminal conduct or activity, and
  - The LPR information is relevant to that suspected criminal conduct or activity and the requestor has a legitimate need to know.

Authorized uses are described in A.2 of this policy. However, the **[name of entity]** accords special consideration to the collection of LPR information relating to First Amendment-protected events and will articulate a legal or justified basis for such collection during the planning assessment and approval process for the particular event, before proceeding with the collection.[2]

2. The **[name of entity]** will prohibit access, use, or dissemination of LPR information for:

- Any purpose that violates the Constitution or laws of the United States, including the protections of the Fourth Amendment.
- Non-law enforcement or personal purposes.
- Discriminatory 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.[3]
- The purpose of prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by and secured by the U.S. Constitution or any other constitutionally protected right or attribute.
- 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, noted in Section E.4.
- Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

3. In addition, the **[name of entity]** will employ credentialed, role-based access criteria, as appropriate, to control:

   - The LPR information to which a particular group or class of users may have access based on the group or class.
   - The assignment of roles (e.g., administrator, manager, operator, and user).
   - The categories of LPR information that a class of users are permitted to use in order to update a hot list, including information being utilized in specific investigations.
   - Any administrative or functional access required to maintain, control, administer, audit, or otherwise manage the information or equipment.

G. Sharing and Dissemination of LPR Information

1. The **[name of entity]** will establish requirements for any external agency requesting access to the **[name of entity]**'s LPR information. These requirements will be documented in an interagency agreement/memorandum of understanding and will include an assurance from the external agency that it complies with the laws and rules governing those individual agencies, including applicable federal and state laws.

2. The **[name of entity]**'s LPR information **will not** be:

   - Sold, published, exchanged, or disclosed to commercial or private entities or individuals except as required by applicable law and to the extent authorized by the **[name of entity]**'s agreement with a commercial vendor.
   - Disclosed or published without prior notice to the originating entity that such information is subject to disclosure or publication. However, the **[name of entity]** and the originating agency may agree in writing in advance that the **[name of entity]** will disclose LPR information as part of its normal operations, including disclosure to an external auditor of the LPR information.
   - Disclosed on a discretionary basis unless the originating agency has provided prior written approval or unless such disclosure is otherwise authorized by the memorandum of understanding or agreement between the **[name of entity]** and the originating agency.
   - Disclosed to unauthorized individuals.

3. The **[name of entity]** will not confirm the existence or nonexistence of LPR information to any individual or agency that would not be authorized to receive the information unless otherwise required by law.

H. Information Quality Assurance

1. Original LPR 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.

2. Whenever a license plate reader alerts on license plate information, prior to taking any law enforcement action, officers will be required, to the fullest extent possible, to visually verify that the actual vehicle license plate information matches the license plate information used and alerted upon by the LPR system, including both alphanumeric characters of the license plate and the state of issuance; verify the current status of the plate as active through **[insert name of source, such as mobile information terminal [MDT] query, NCIC, etc.]**; and confirm whether the alert pertains to the registrant of the car or the car itself. Receipt of an LPR alert for a stolen or felony vehicle may not rise to the level of reasonable suspicion and is not sufficient probable cause to arrest without confirmation that the alert is still valid and active. If the alert is for another type of transaction, the officer will read the description of the alert and follow the appropriate action or reporting method. If an LPR alert cannot be verified both visually and for validity, then law enforcement should not act on the alert and it should be rejected.

   If the officer witnesses a violation of law or other action that establishes reasonable suspicion for a stop, the officer may conduct a stop based on that reasonable suspicion. This provision shall not prevent a law enforcement officer from taking immediate action when a verifiable emergency situation exists for officer safety.

   On each resulting alert, the officer is required to enter a disposition indicating the action taken or not taken on the alert.

3. The **[name of entity]** will perform routine maintenance, upgrades, calibration, and refreshes of all LPR equipment and components to ensure proper functionality, including the following:

   - At the beginning of a shift, officers will visually inspect the exterior cameras to ensure the lenses are clear and the cameras have not been altered in any way.

- Designated, trained personnel shall check LPR equipment on a regular basis to ensure functionality and proper camera alignment.
- Any equipment that falls outside expected functionality shall be removed from service until deficiencies have been corrected.
- Officers will not attempt to disconnect, modify, or change the LPR equipment or software unless authorized to do so.
- Damage or other malfunctions to the equipment will be reported to the **[insert position/title]**.
- The LPR equipment and components will not be transferred to another vehicle except with the prior, written approval of the LPR Administrator.

4. The **[name of entity]** will investigate, in a timely manner, alleged errors and deficiencies of LPR information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and deficiencies.

5. The **[name of entity]** will correct, notate, delete, or refrain from using LPR information the **[name of entity]** originated and found to be erroneous or deficient. Originating agencies external to the **[name of entity]** are responsible for reviewing the quality and accuracy of the LPR information provided to the **[name of entity]** and must take reasonable steps to correct or amend the information upon learning that it is inaccurate or deficient. The **[name of entity]** will review the quality of LPR information it has received from an originating agency or vendor and will advise the appropriate point of contact, in writing or electronically, when its LPR information is alleged, suspected, or found to be erroneous or deficient.

6. The **[name of entity]** will use written or electronic notification to inform recipient agencies **[or, if applicable, use the phrase "inform the consolidated system"]** when LPR information previously provided is erroneous or deficient. In addition, the **[name of entity]** will take reasonable steps to correct or amend the information provided to the external agency in order to ensure accuracy and sufficiency to the extent possible.

I. Redress

I. 1 Disclosure

1. LPR information will be disclosed to the public in accordance with **[cite applicable public records laws]**. **[If your state law permits disclosure, revise provision to reflect this.]**

2. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity, an individual is entitled to know the existence of and to review the LPR information about him or her that has been collected or received and retained by the **[name of entity]**. If allowed by state law, the individual may obtain a copy of the LPR information for the purpose of challenging the accuracy or completeness of the information (correction). The **[name of entity]**'s response to the request for LPR information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests.

I. 2 Corrections

1. If, in accordance with state law, an individual requests correction of LPR information *originating with the* **[name of entity]** that has been disclosed, the **[name of entity]**'s **[insert title of designee]** will inform the individual of the procedure for requesting corrections, including appeal rights for those requests that are denied in whole or in part. A record will be kept of all requests.

I. 3 Appeals

1. The individual who has requested disclosure or to whom LPR information has been disclosed will be informed of the reason(s) why the **[name of entity]** or originating agency denied the request for disclosure or correction. The individual will also be informed of the procedure for appeal when the **[name of entity]** or originating agency has cited an exemption for the type of information requested or has declined to correct challenged LPR information to the satisfaction of the individual to whom the information relates.

J. Security and Maintenance

1. The **[name of entity and, if applicable, the name of entity's LPR vendor]** will operate in a secure facility protected from external intrusion and will utilize secure internal and external safeguards against network intrusions. Access to **[name of entity]** LPR information from outside the facility will be allowed only over secure networks.

2. All LPR equipment, software, and components will be properly maintained in accordance with the manufacturer's recommendations and/or any published industry standards.

3. The **[name of entity or, if applicable, the name of entity's LPR vendor]** will store LPR information in a manner that ensures that it cannot be added to, modified, accessed, or purged except by personnel authorized to take such actions.

4. Access to **[name of entity]** LPR 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.

5. Usernames and passwords to LPR information are not transferrable, must not be shared by **[name of entity]** personnel, and must be kept confidential.

6. User passwords must meet the following standards **[insert rules, such as no English words and a combination of letters, numbers, and at least two symbols]**. The system administrator will ensure that all manufacturer-generated default passwords are replaced with secure passwords before web-based interfaces of the system become operational.

7. Queries made to the **[name of entity]**'s LPR 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.

8. The **[name of entity]** will maintain an audit trail of accessed, requested, or disseminated **[name of entity]**-held LPR information. An audit trail will be kept for a minimum of **[specify the retention period for your jurisdiction/entity for this type of request]** of requests for access to LPR information for specific purposes and of what LPR information is disseminated to each individual in response to the request. Audit logs will include:

   - The name and agency of the law enforcement user.
   - The date and time of access.
   - The specific information accessed.
   - The modification or deletion, if any, of the LPR information.
   - The authorized law enforcement or public safety justification for access, including a relevant case number if available.

9. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

10. **Option 1: State Information Breach Law**

    The **[name of entity]** will follow the information breach notification guidance set forth in **[cite to applicable law]**. **[To the extent required by the (state) information breach notification law, add:]** The **[name of entity]** will immediately notify the originating agency from which the **[name of entity]** received personal information of a suspected or confirmed breach of such information.

    Option 2: No State Information Breach Law

    A: Entity Follows Guidance From the Office of Management and Budget (OMB)
    The **[name of entity]** will follow the information breach notification guidance set forth in OMB Memorandum M-07-16 (May 2007), available at http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf.

    B: Entity Adheres to the Following Policy
    [If there is no applicable state information breach notification law.] The **[name of entity]** will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the individual. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or take any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

K. Information Retention and Purging

1. All LPR information contained within the **[name of entity]**'s LPR system will be stored for a period not to exceed **[insert a time frame]**. After **[insert time period]**, the information will be automatically purged (i.e., permanently removed from the system).

This retention policy applies only to the LPR information contained in the **[name of entity]**'s LPR system itself. Once an LPR record is downloaded by **[name of entity]** personnel and incorporated into a criminal intelligence record or investigative case file, the LPR information is then considered intelligence or investigative information and the laws, regulations, and policies applicable to that type of information or intelligence govern its use.

If the LPR record has become or there is reason to believe that it will become evidence, including evidence that tends to inculpate or exculpate a suspect, in a specific criminal or other law enforcement investigation or action, the following provisions apply:

a. In those circumstances in which an LPR record is identified as having evidentiary value, the LPR **[insert Administrator or other title]** or designee will review the facts of the specific case and determine whether the information should be retained beyond the established retention period. If it is determined that it is reasonable to believe the information has evidentiary value, the LPR **[insert Administrator or other title]** will authorize the transfer of the applicable record from the LPR system server to **[insert appropriate response; for example, "the entity's case management system" or "a form of digital storage media (CD, DVD, etc.) or other portable storage device"]**.
b. Agencies requiring LPR records to be retained by the **[name of entity]** beyond the established retention period may make a formal, written request to the **[name of entity]** to extend retention. Each request must specify the need for extended retention, the circumstances surrounding the request, the requesting agency's case number, and a specific point of contact within the requesting agency. The **[name of entity]** reserves the right to grant or deny agency requests based on the information provided.

The **[name of entity]** retains the right to remove LPR information earlier than the retention period, based on limitations of information storage requirements and subject to applicable statutory disclosure mandates. Early removal, however, will not be used as a means for intentionally interfering with a lawful complaint or a public records request. The retention period may be modified at any time by the **[name of entity]**, subject to applicable legal requirements.

L. Accountability and Enforcement

L.1. Transparency

1. The **[name of entity]** will be open with the public in regard to LPR information collection, receipt, access, use, dissemination, retention, and purging practices. The **[name of entity]**'s LPR policy will be made available in printed copy upon request and posted prominently on the **[name of entity]**'s Web site **[or Web page]** at **[insert Web address]**.

2. The **[name of entity]**'s **[Privacy Officer, LPR Administrator, or other position title]** will be responsible for receiving and responding to inquiries and complaints about incorrect information or privacy, civil rights, and civil liberties protections in the LPR information system maintained or accessed by the **[name of entity]**. The **[Privacy Officer, LPR Administrator, or other position title]** may be contacted at **[insert mailing address or e-mail address]**.

L.2. Accountability

1. The **[name of entity]** will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this LPR policy and applicable law. This will include logging access to LPR information and periodic random auditing of these systems, so as not to establish a discernable pattern that may influence users' actions. These audits will be mandated at least **[insert quarterly, semiannually, annually, or other time period]**, and a record of the audits will be maintained by the **[Privacy Officer, LPR Administrator, or title of designee]** of the **[name of entity]**. Audits may be completed by an independent third party or a designated representative of the **[name of entity]**.

Appropriate elements of this audit process and key audit outcomes will be compiled into a report and may be provided to command staff and oversight entities or governance boards.[4]

[Entities may also release the results of the audit to the public, pursuant to law or as a matter of discretion. Under these circumstances, consider the following options.]

Option 1: The **[name of entity]** will provide, at minimum, an overview to the public to enhance transparency with respect to privacy, civil rights, and civil liberties protections built into the **[name of entity]**'s operations.

Option 2: The **[name of entity]** will also release to the public the full audit, with redactions as necessary to protect the privacy of any individual or group, if appropriate and consistent with jurisdictional requirements.

2. The **[name of entity]**'s personnel or other authorized users shall report errors and suspected or confirmed violations of the **[name of entity]**'s LPR policy to the **[name of entity]**'s **[insert title of LPR Administrator]**.

3. The **[Privacy Officer, LPR Administrator, or other position title]** will review and update the provisions contained in this LPR policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the LPR system; the audit review; and public expectations.

L.3. Enforcement

1. If **[name of entity]** personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, receipt, access, use, dissemination, retention, and purging, the **[title of entity Director]** of the **[name of entity]** will:

   - Suspend or discontinue access to information by the **[name of entity]** personnel, the participating agency, or the authorized user;
   - Apply appropriate disciplinary or administrative actions or sanctions;
   - If the authorized user is from an agency external to the **[name of entity]**, request that the user's employer initiate disciplinary proceedings to enforce the policy's provisions; and/or
   - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

2. The **[name of entity]** reserves the right to establish the qualifications and number of personnel having access to **[name of entity]** LPR information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating this LPR policy.

M. Training

1. Before access to **[name of entity]** LPR information is authorized, the **[name of entity]** will require the following individuals to participate in training regarding implementation of and adherence to this LPR policy:

   - All authorized **[name of entity]** personnel.
   - All authorized participating agency personnel.
   - All authorized personnel providing information technology services to the **[name of entity]**.

2. The **[name of entity]**'s LPR policy training program will cover:

   - Purposes of the LPR policy.
   - Substance and intent of the provisions of this LPR policy, and any revisions thereto, relating to collection, receipt, access, use, dissemination, retention, and purging of the **[name of entity]**'s LPR information and the privacy, civil rights, and civil liberties protections on the use of the technology and the information collected or received.
   - Appropriate procedures relating to license plate image quality and mitigating the risks associated with a possible misread by the LPR system.
   - LPR verification process for law enforcement alerts.
   - Originating and participating agency responsibilities and obligations under applicable federal, state, or local law and policy.
   - How to implement the LPR policy in the day-to-day work of the user, whether a paper or systems user.
   - Mechanisms for reporting violations of **[name of entity]** LPR policy provisions.
   - The nature and possible penalties for LPR policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

[1] Refer to state law regarding ownership and compliance with open record requests regarding LPR information.

[2] For further information about these processes, see *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies* at 4, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.
[3] Ibid. at 6–7 and 11–13.
[4] *Privacy, Civil Rights, and Civil Liberties Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component*, Global Justice Information Sharing Initiative, https://it.ojp.gov/GIST/181/Privacy--Civil-Rights--and-Civil-Liberties-Audit-Guidance-for-the-State--Local--Tribal--and-Territorial-Intelligence-Component.

MHQ
VEHICLES ■ EQUIPMENT ■ GEAR

QUOTE

CUSTOMER

Contact Name:	Brian Egnitz	Date:	3/23/2017
Company/Dept:	Massachusetts State Police - Commonwealth Fusion Center	Valid for:	60 Days*
Street Address:			
City, State, Zip:		Contract #:	SP16-MSPVEH-F80
Phone:	978-451-3710; 508-988-7216	Sales Rep:	Kris Wright
E-Mail:	brian.egnitz@state.ma.us		

PRODUCT	PRODUCT DESCRIPTION	UNIT PRICE	QTY.	EXTENDED PRICE
75030254587	**3M™ Plate Alert Analytics 1 YR**	[redacted]		$11,280.00
75030254546	**3M™ Plate Alert Basic 1 YR for 41-100 devices**			$42,300.00
75030254579	**3M™ Plate Alert Pattern 1 YR**			$8,460.00
75030235792	**P492 750NM 50/35 8GB W/HOOD** The 3M™ Fixed Wide Lane ALPR Camera P492 captures multiple license plates in the same field of view across 13.6 feet of US freeway traffic lanes. It is designed to utilize smaller, high power LEDs and provides the best color overview image resolution offered by 3M™ ALPR cameras.			$310,200.00
	UL Listed 15V Power Supply Camera Interface Module 15V Provides 15V power, Ethernet and RS232 connections to P392 Cameras. Designed to fit into the 3M ALPR interface boxes listed above. Bottom bracket may be removed for installation of customer provided DIN rail mounting clip for customer cabinet mounting.			$21,150.00
75030222303	**UNIVERSAL FIXED BRKTS (P392+/P492/P382)** Accessories for ALPR fixed cameras			$23,970.00
	Shipping and Handling			$2,250.00
			TOTAL:	**$419,610.00**

TERMS AND CONDITIONS

*This quote is valid for 60 days from the date of quote. Any purchase orders or approved quotes received outside of the 60 day quote period will be subject to price adjustments. By signing this quote, the customer is agreeing to pay, in full, for all items listed above. Any requests for changes, modifications, replacements, removals or additional items may be subject to additional fees and/or adjusted delivery dates.

The terms and conditions stated herein and the provisions of any agreement between MHQ and Buyer, if applicable, shall constitute the complete and only terms and conditions applicable to any and all purchases by Buyer from MHQ. Any additional and/or different terms and/or conditions printed anywhere including on, or with, Buyer's order shall be inapplicable in regard to any purchase by Buyer from MHQ.

ORDER ACKNOWLEDGEMENT

By signing this document you are agreeing to the above terms and conditions of this order from MHQ, Inc.

x _____

PRINT NAME

x _____

TITLE

x _____

SIGNATURE

Quote provided by Kris Wright, Account Manager at MHQ
(508) 573-2618 or kwright@mhq.com

MHQ
VEHICLES ■ EQUIPMENT ■ GEAR

QUOTE

CUSTOMER

Contact Name:	Brian Egnitz	Date:	3/23/2017
Company/Dept:	Massachusetts State Police - Commonwealth Fusion Center	Valid for:	60 Days*
Street Address:			
City, State, Zip:		Contract #:	SP16-MSPVEH-F80
Phone:	978-451-3710; 508-988-7216	Sales Rep:	Kris Wright
E-Mail:	brian.egnitz@state.ma.us		

PRODUCT	PRODUCT DESCRIPTION	UNIT PRICE	QTY.	EXTENDED PRICE
75030254587	**3M™ Plate Alert Analytics 1 YR**	[redacted]		$11,280.00
75030254546	**3M™ Plate Alert Basic 1 YR for 41-100 devices**			$14,100.00
75030254579	**3M™ Plate Alert Pattern 1 YR**			$8,460.00
75030235792	**P492 750NM 50/35 8GB W/HOOD** The 3M™ Fixed Wide Lane ALPR Camera P492 captures multiple license plates in the same field of view across 13.6 feet of US freeway traffic lanes. It is designed to utilize smaller, high power LEDs and provides the best color overview image resolution offered by 3M™ ALPR cameras.			$310,200.00
	UL Listed 15V Power Supply Camera Interface Module 15V Provides 15V power, Ethernet and RS232 connections to P392 Cameras. Designed to fit into the 3M ALPR interface boxes listed above. Bottom bracket may be removed for installation of customer provided DIN rail mounting clip for customer cabinet mounting.			$21,150.00
75030222303	**UNIVERSAL FIXED BRKTS (P392+/P492/P382)** Accessories for ALPR fixed cameras			$23,970.00
	Shipping and Handling			$2,250.00
			TOTAL:	**$391,410.00**

TERMS AND CONDITIONS

*This quote is valid for 60 days from the date of quote. Any purchase orders or approved quotes received outside of the 60 day quote period will be subject to price adjustments. By signing this quote, the customer is agreeing to pay, in full, for all items listed above. Any requests for changes, modifications, replacements, removals or additional items may be subject to additional fees and/or adjusted delivery dates.

The terms and conditions stated herein and the provisions of any agreement between MHQ and Buyer, if applicable, shall constitute the complete and only terms and conditions applicable to any and all purchases by Buyer from MHQ. Any additional and/or different terms and/or conditions printed anywhere including on, or with, Buyer's order shall be inapplicable in regard to any purchase by Buyer from MHQ.

ORDER ACKNOWLEDGEMENT

By signing this document you are agreeing to the above terms and conditions of this order from MHQ, Inc.

x _____

PRINT NAME

x _____

TITLE

x _____

SIGNATURE

Quote provided by Kris Wright, Account Manager at MHQ
(508) 573-2618 or kwright@mhq.com

3M Science. Applied to Life.™

3M Center, Bldg 225-4N-14
St. Paul, MN 55144-1000
P: 1-877-777-3571
E: 3mtssdorders@mmm.com

Quote Number	00011716	Created Date	3/22/2017
Quote Name	P492 Fixed Camera + Plate Alert Software	Expires On	6/20/2017
Prepared By	John Tedona	Contact Name	Brian Egnitz
Phone	1-201-841-6237	Email	brian.egnitz@state.ma.us
Email	jtedona@mmm.com		
Bill To Name	STATE OF MASSACHUSETTS DEPT OF STATE POLICE	Ship To Name	STATE OF MASSACHUSETTS DEPT OF STATE POLICE
Bill To	490 WORCESTER RD FRAMINGHAM, Massachusetts 01702 United States		

Quantity	Product Code	Product	Product Description	List Price	Total Price	Total S & H
[redacted]	030254587	3M™ Plate Alert Analytics 1 YR		[redacted]	USD 12,000.00	USD 0.00
	030254546	3M™ Plate Alert Basic 1 YR for 41-100 devices			USD 15,000.00	USD 0.00
	030254579	3M™ Plate Alert Pattern 1 YR			USD 9,000.00	USD 0.00
	030235792	P492 750NM 50/35 8GB W/HOOD	The 3M™ Fixed Wide Lane ALPR Camera P492 captures multiple license plates in the same field of view across 13.6 feet of US freeway traffic lanes. It is designed to utilize smaller, high power LEDs and provides the best color overview image resolution offered by 3M™ ALPR cameras.		USD 330,000.00	USD 2,250.00
		UL Listed 15V Power Supply Camera Interface Module 15V	Provides 15V power, Ethernet and RS232 connections to P392 Cameras. Designed to fit into the 3M ALPR interface boxes listed above. Bottom bracket may be removed for installation of customer provided DIN rail mounting clip for customer cabinet mounting.		USD 22,500.00	USD 0.00
	030222303	UNIVERSAL FIXED BRKTS (P392+/P492/P382)	Accessories for ALPR fixed cameras		USD 25,500.00	USD 0.00

Total Price	USD 414,000.00
Shipping and Handling	USD 2,250.00
Grand Total	USD 416,250.00

Terms: Net 30 days
F.O.B. Freight will be prepaid by 3M and billed to customer
Shipping Costs: 3M to prepay and add to invoice
Warranty: One year return-to-depot included with purchase

Conditions of This Sale:

- Prices quote herein are firm fixed prices for your project and are valid for 90 days, unless otherwise specified.

3M Center, Bldg 225-4N-14
St. Paul, MN 55144-1000
P: 1-877-777-3571
E: 3mtssdorders@mmm.com

- Pricing is based on supplying the designated item(s) shown. Any changes in quantities or item descriptions will require new pricing to evaluate the Quotation without written consent from 3M Traffic Safety and Security Division.
- The prices quoted exclude any applicable taxes and duties, including local sales taxes
- 3M reserves the right to revise this Quotation in the event that any of the terms and conditions set forth are varied.
- An estimated delivery date range will be provide for all non-budgetary quotes. Due to resourcing requirements and the nature of the identity management business the delivery estimates are subject to change.
- Additional 3M terms and Conditions of Sales are attached

Information for PO:

- Provide your corporate Tax ID number or Tax Exempt Certificate
- 'Ship To', 'Bill To', Deliver to Contact Name and Phone Number
- Acknowledgement of shipping and handling to be added to Invoice at time of shipment and/or charge freight collect against customer's account (provide account #)

Terms and Conditions of Sale

These Terms and Conditions of Sale ("Terms") apply to every order ("Order") of products or services ("Products") by 3M Traffic Safety and Security Division ("3M"). 3M's acceptance of each Order is expressly conditioned on the Buyer's acceptance of all the Terms. If any 3M proposal is construed as an offer, that offer is expressly limited by these Terms. Any notice of different or additional terms, including, without limitation, any terms on a Buyer's purchase order, or any Buyer notice of rejection of the Terms, is hereby rejected. If any 3M action regarding a proposal from Buyer, including 3M's shipment of Products, is construed as an acceptance of Buyer's offer, such acceptance is expressly conditioned on Buyer's acceptance of these Terms.

1. Pricing and Shipping: Pricing is as provided in the 3M quotation or applicable 3M price page ("Quotation"). Prices quoted by 3M are valid for 90 days after the date of the Quotation. Any changes in quantity or release dates may result in a change in pricing. Prices are F.O.B. point of shipment and exclude shipping, taxes, and any applicable duties.

2. Payment Terms: Payment terms are net 30 days from the date of 3M invoice.

3. Credit: 3M may, in its sole discretion at any time, change or limit the amount or duration of credit extended to the Buyer. 3M may cancel any Orders or delay shipment of an Order, if the Buyer fails to meet payment schedules or other credit or financial requirements established by 3M.

4. Lead Times: Delivery lead times will be quoted at the time of Order. 3M will use reasonable efforts to ship within quoted lead times, but is not liable for delivery delays.

5. Returned Goods Policy: Returns are subject to 3M's then current Returned Goods Policy. In all instances, authorization must be received from your 3M customer service representative before any returns will be accepted.

6. Export Control Compliance: Products are delivered within the United States. The ultimate destination of any Products purchased for export or re-export must be disclosed to 3M at the time of order. Buyer is responsible for complying with all applicable export control laws.

7. Product Selection and Use: The technical information, recommendations and other statements relating to the Products are based upon tests or experience that 3M believes are reliable, but the accuracy or completeness of such information is not guaranteed. Many factors beyond 3M's control and uniquely within Buyer's knowledge and control can affect the use and performance of a Product in a particular application Given the variety of factors that can affect the use and performance of a Product, Buyer is solely responsible for evaluating the 3M product and determining whether it is fit for a particular purpose and suitable for Buyer's method of application.

8. Confidentiality: Any information supplied by 3M in response to Buyer's request for quotation will not be used for any purpose other than to evaluate 3M's proposal and, except as required by law, may be not be disclosed or used for any other purpose.

9. Warranty and Limited Remedy: THE FOLLOWING IS MADE IN LIEU OF ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. 3M warrants that its 3M Security Systems Division products will meet 3M's written specifications at the time of shipment. 3M's obligation and your exclusive remedy shall be, at 3M's option, to replace or repair the 3M product or refund the purchase price of the 3M product. IN NO EVENT WILL 3M BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES INCLUDING, BUT NOT LIMITED TO LOSS OF PROFITS, IN ANY WAY RELATED TO THE PRODUCTS REGARDLESS OF THE LEGAL THEORY ASSERTED.

10. Federal Contracts: 3M is selling commercial items as defined in FAR 2.101. If an Order is issued under a Federal Government contract or higher-tier subcontract, the following additional terms and conditions apply to the extent that the terms and conditions are applicable based on their FAR or DFARS prescriptions for commercial item procurements, as of the date of the Order: FAR 52.212-5(e) when the buyer's government contract is for commercial items or services, FAR 52.244-6 when the buyer's government contract is for noncommercial items/services, and additionally, DFARS 252.212-7001(c) when the buyer's contract is with the Department of Defense.

The FAR and DFARS specify that for the acquisition of commercial items, prime contractors (Buyer) are not required to flow down any FAR clauses other than those listed above. Therefore, acceptance of any order placed by Buyer does not constitute acceptance by 3M of any other government contract provision other than those listed above, regardless of terms and conditions included on Buyer boilerplate order documents, and any such provisions are expressly rejected as a condition of these Terms.

3M Center, Bldg 225-4N-14
St. Paul, MN 55144-1000
P: 1-877-777-3571
E: 3mtssdorders@mmm.com

11. Changes: 3M reserves the right to amend, modify, or supplement these Terms as to future orders or shipments. No action by Buyer may amend, modify, reject, supplement, or waive these Terms in any manner whatsoever (including course of dealing or of performance or usage of trade) except as agreed upon in a writing signed by an authorized representative of 3M.

12. Waiver: Any failure or delay by either Party in exercising any right or remedy provided by or relating to the Quotation or these Terms in one or more instances does not constitute a waiver and shall not prohibit a Party from exercising such right or remedy at a later time or from exercising any other right or remedy available.

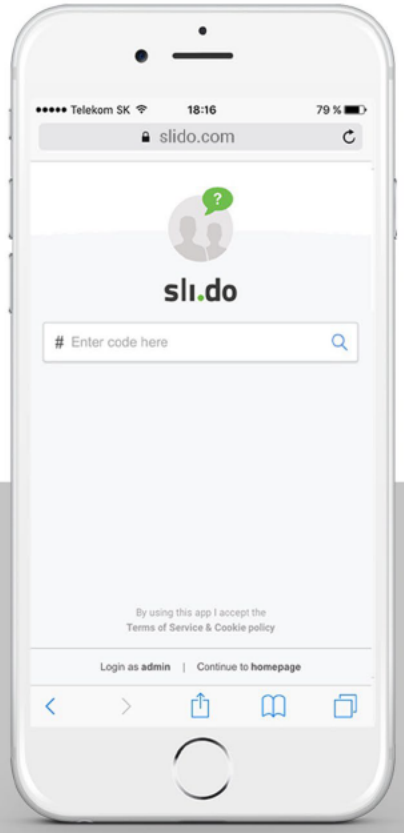
13. Severability: If any provision of the Quotation or these Terms shall, for any reason, be held invalid, illegal, or unenforceable by a court or tribunal of competent jurisdiction, such provision shall be deemed severable and such invalidity, illegality, or unenforceability shall not affect any other provision of the Quotation or these Terms which shall be enforced in accordance with the intent of this Agreement.

14. Complete Agreement: The Quotation and these Terms constitute the entire agreement between the Parties and supersede and terminate any and all prior agreements and understandings, whether written or oral, between the Parties with respect to the subject matter of the Order. Each Party agrees that it has not relied on any representation, warranty, or provision not expressly stated herein and that no oral statement has been made to either Party in any way tends to waive any of the these terms. The UN Convention on the International Sale of Goods shall not apply.

US SGBG TSSD ALPR Direct

Use this app to ask questions during the training!

JOIN THE CONVERSATION



Go to www.slido.com
and insert code:

#5103



Information Sharing Leads to Officer Safety

Teri M. Fournier-Harsin, Nlets Training Manager

2017 Massachusetts State Training

What to Expect

- Ice Breaker / Group Activity
- Overview of Nlets
- Information Sharing Over Nlets
- Parsing
- Resources
  - Message Key Maps



Icebreaker

- Pair Up
- Discuss what you know about Nlets
  - Governmental? Private?
  - Governed by?
  - Purpose?
- Share with the group



We have existed for 50 years to connect all states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, Guam, and Canada along with 28 federal agencies and various associate members for ***the secure exchange of criminal justice data*** necessary to complete our law enforcement, justice, and public safety mission.



Nlets is ***not*** the same as NCIC!

The FBIs NCIC is a ***computerized index of criminal justice information.*** It is available to federal, state, and local law enforcement and other criminal justice agencies.





Nlets is a ***self-funded, private, not-for-profit corporation*** that has created dozens of secure partnerships ***for data exchange.***

We are owned and governed solely by the 54 lead law enforcement agencies that make up the principal customers of Nlets.

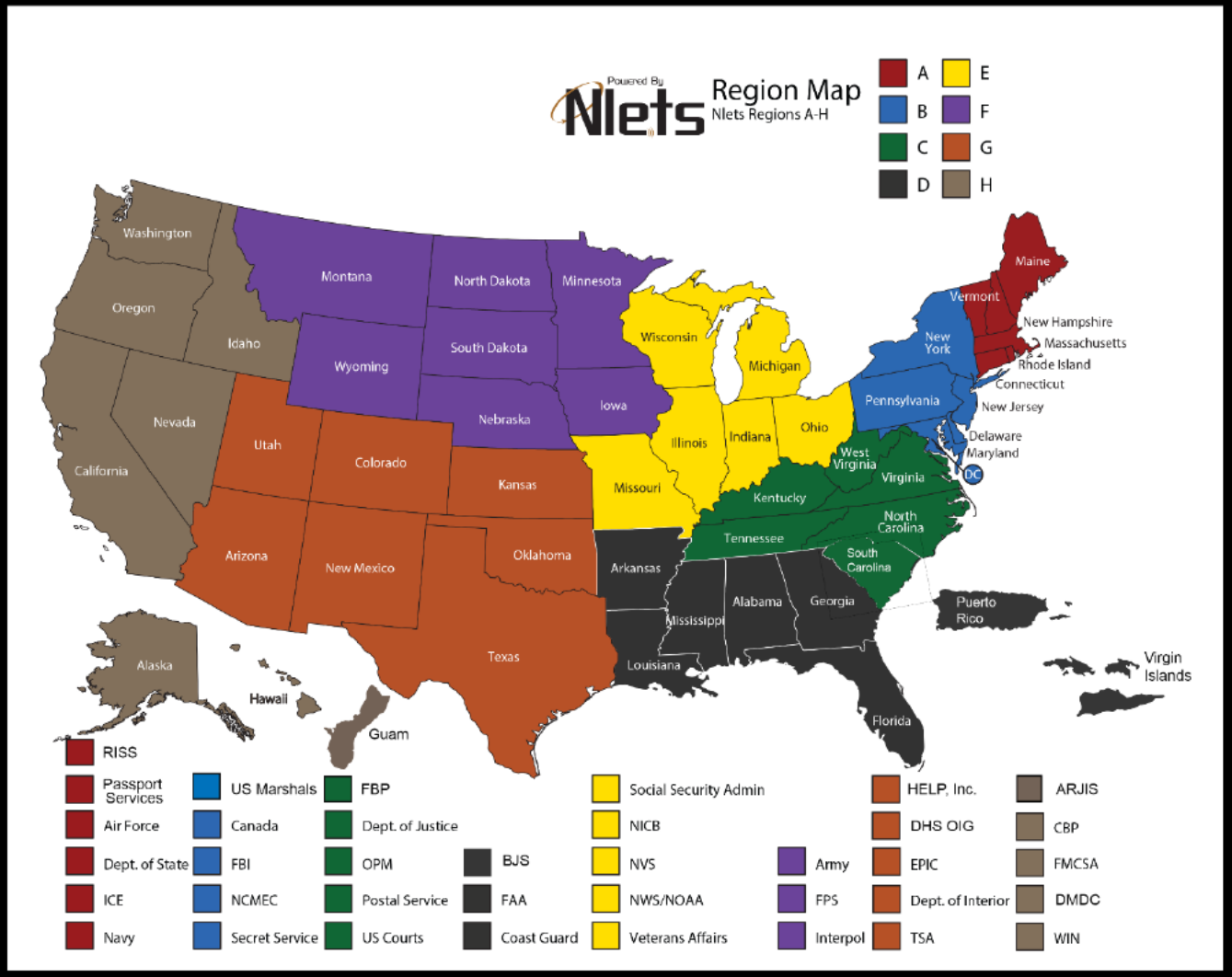


Our membership is represented by one individual per state – this is the ***Nlets Rep***.

The states are divided into eight regions. Each region elects a chairperson to represent the region on the ***Nlets Board of Directors***.

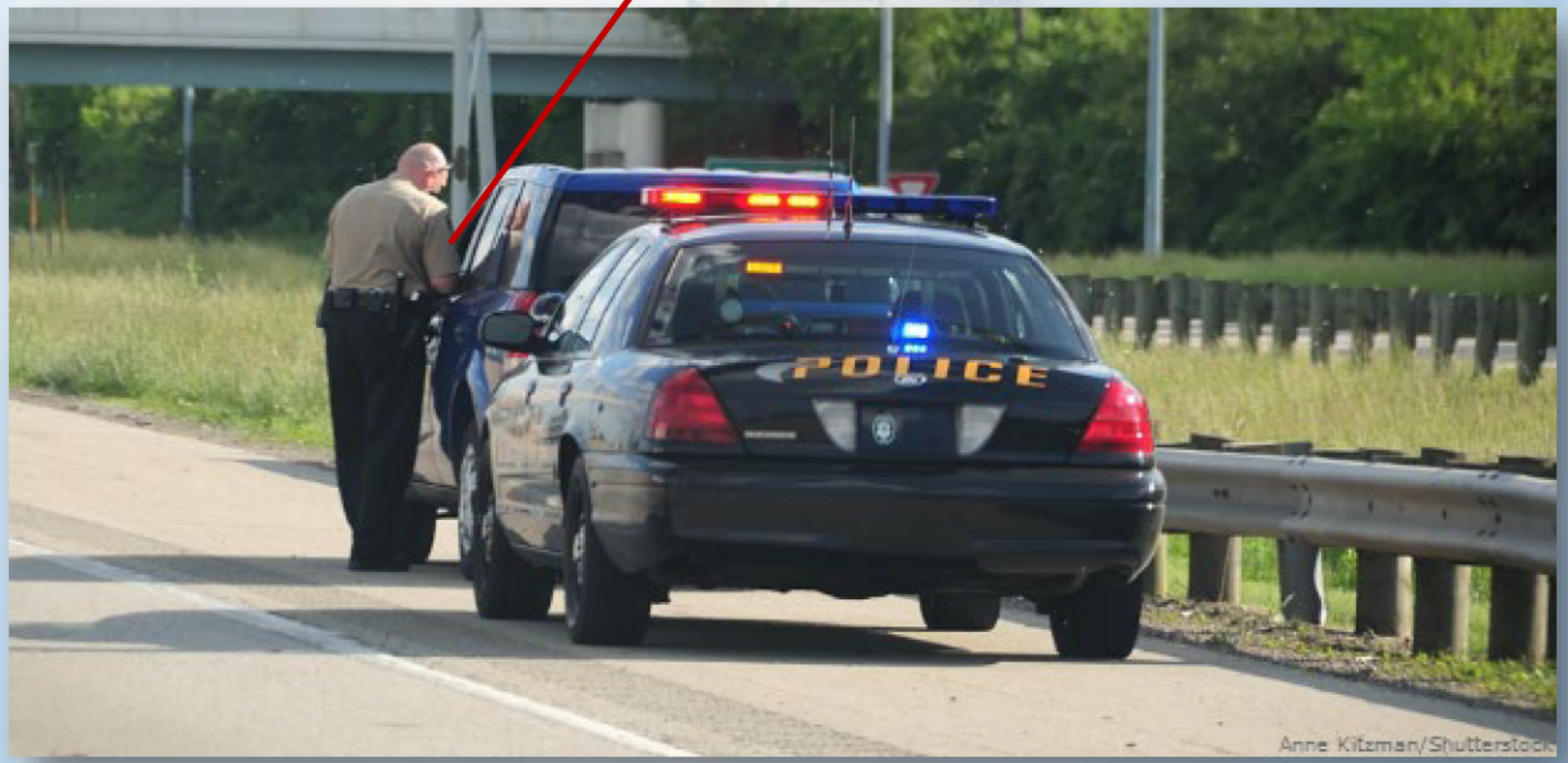
Curt Wood

- *Nlets Rep*
- *Nlets Region A Chair*
- *F&M Committee*
- *Nominations Committee*
- *Hall of Fame Committee*



How Nlets Works

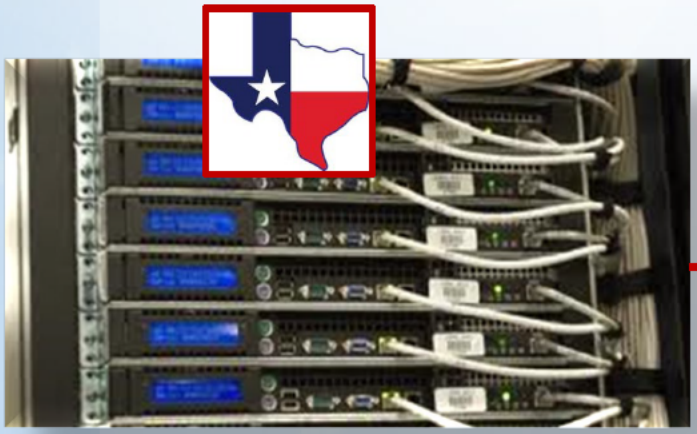




Nlets receives the query from Minnesota, checks to make sure it is a valid request, then forwards the request to Texas.



Texas receives the query, checks the info needed by the out-of-state trooper, and sends an automated response back to Nlets.



Powered By Nlets

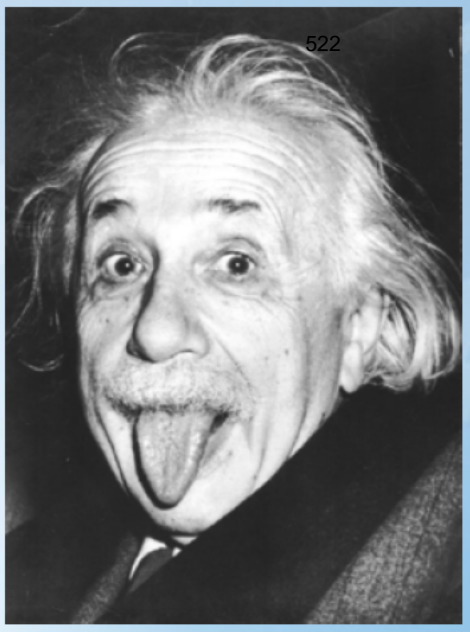


All of this takes place in approximately 1.5 seconds!!

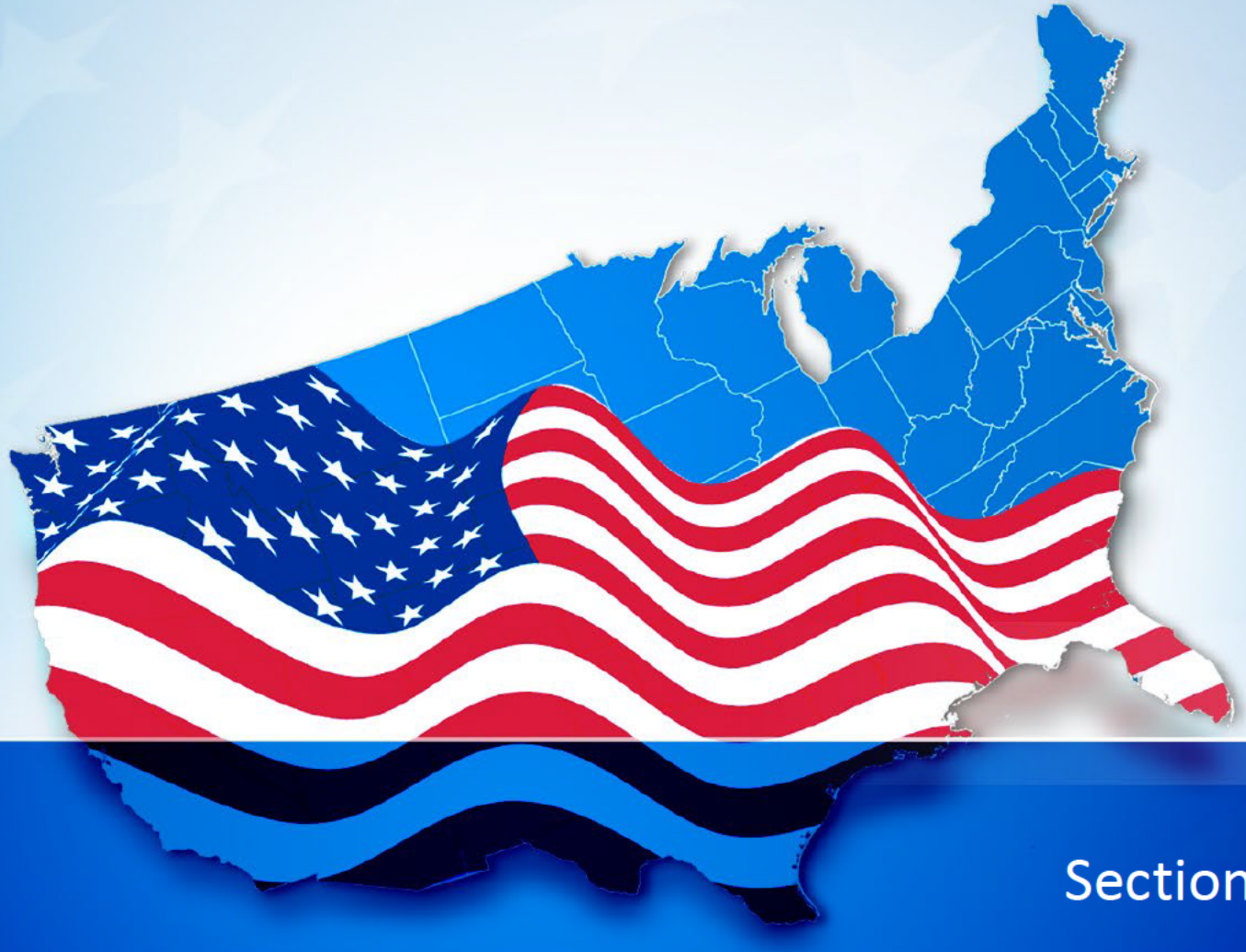
Nlets receives the response from Texas and forwards the information back to Minnesota.







Information Sharing



Section 46 Nlets WIKI

TASER Transactions

Powered By Nlets





Provides access to their database of purchased and registered TASER cartridges in real-time.

Please note that ***law enforcement records*** will be redacted from this service.



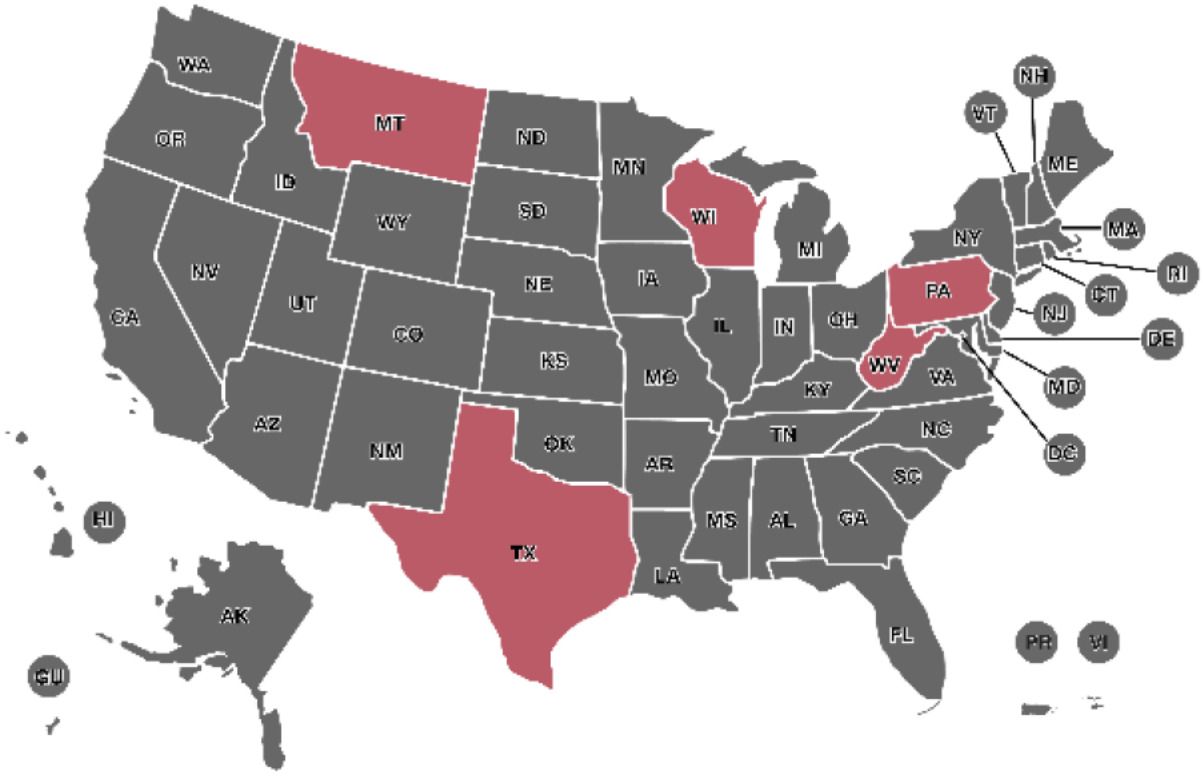


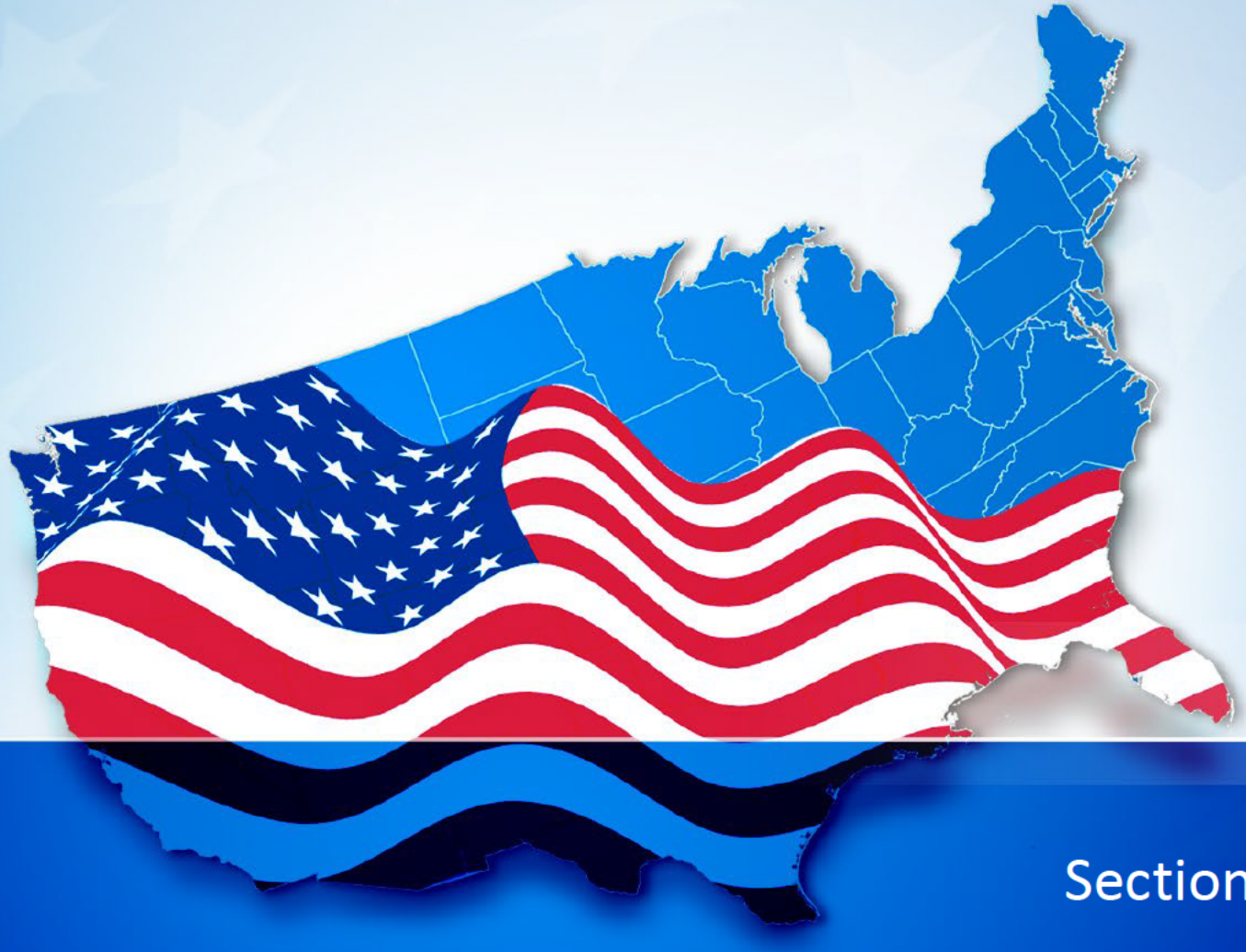
Law enforcement records may still be required during investigations so you can contact TASER and request them:
nletsdatarequest@taser.com



Message Keys: **TASER Registration Query (TSQ)**

Configured to Send this Query





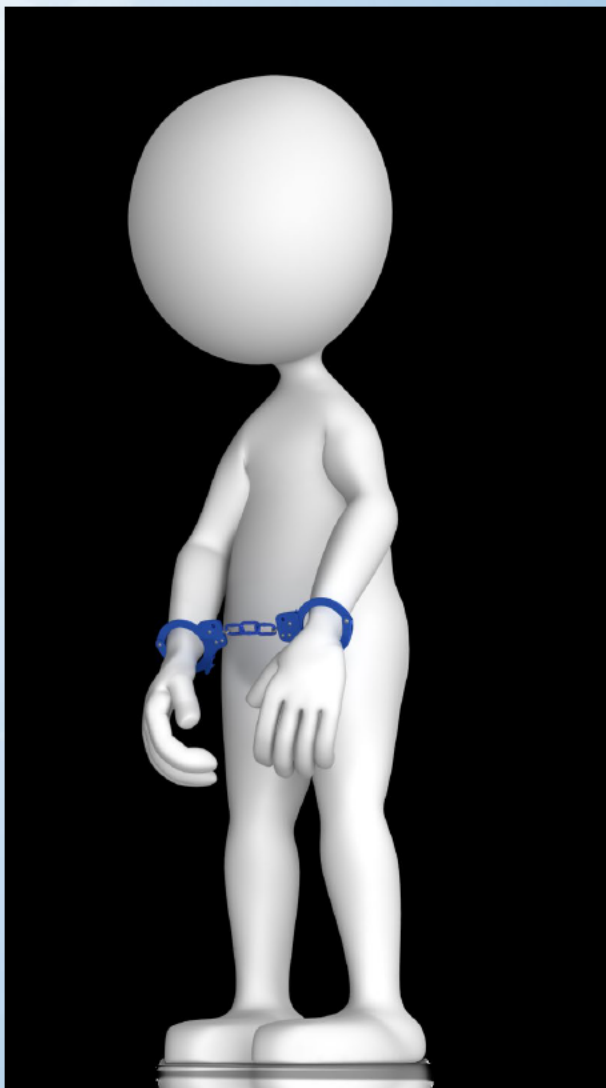
Section 17 Nlets WIKI

Parole, Probation, Corrections

Powered By Nlets



You are able to request out-of-state parole, probation, and corrections information via Nlets.

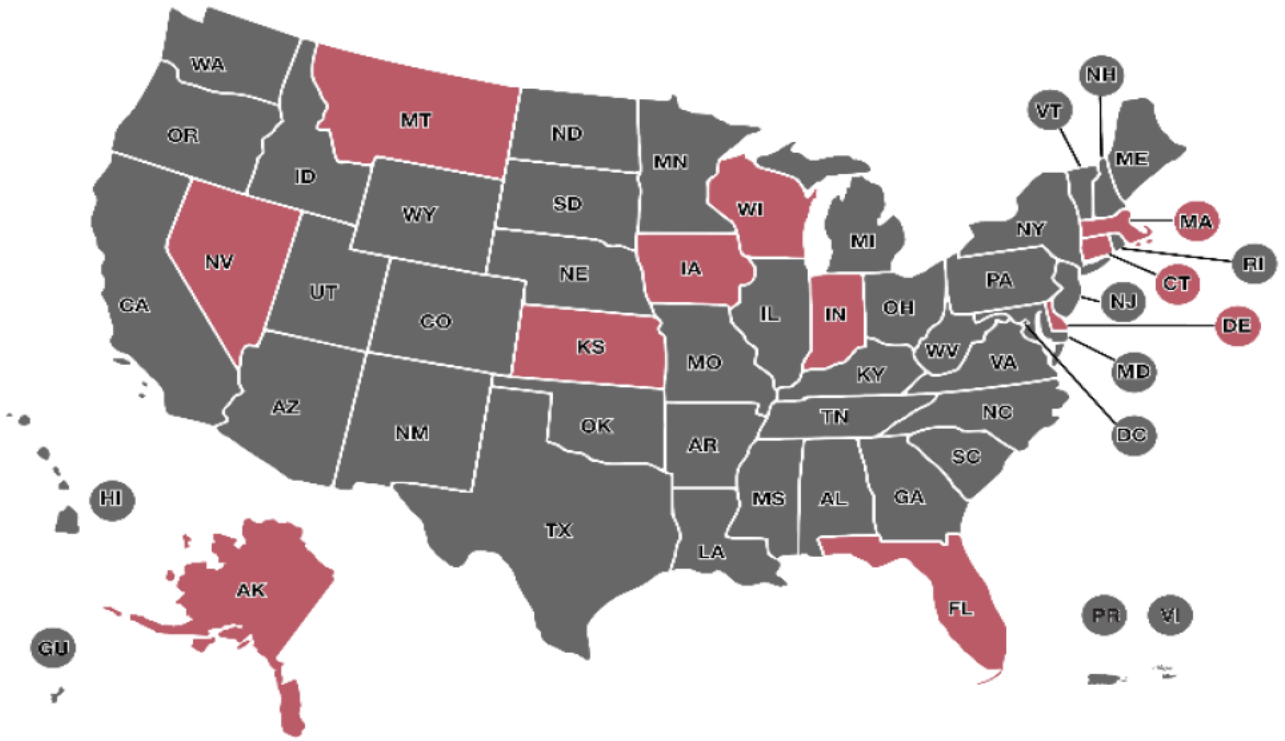


It is important to recognize that some states will not be able to respond to a query on all of these files.



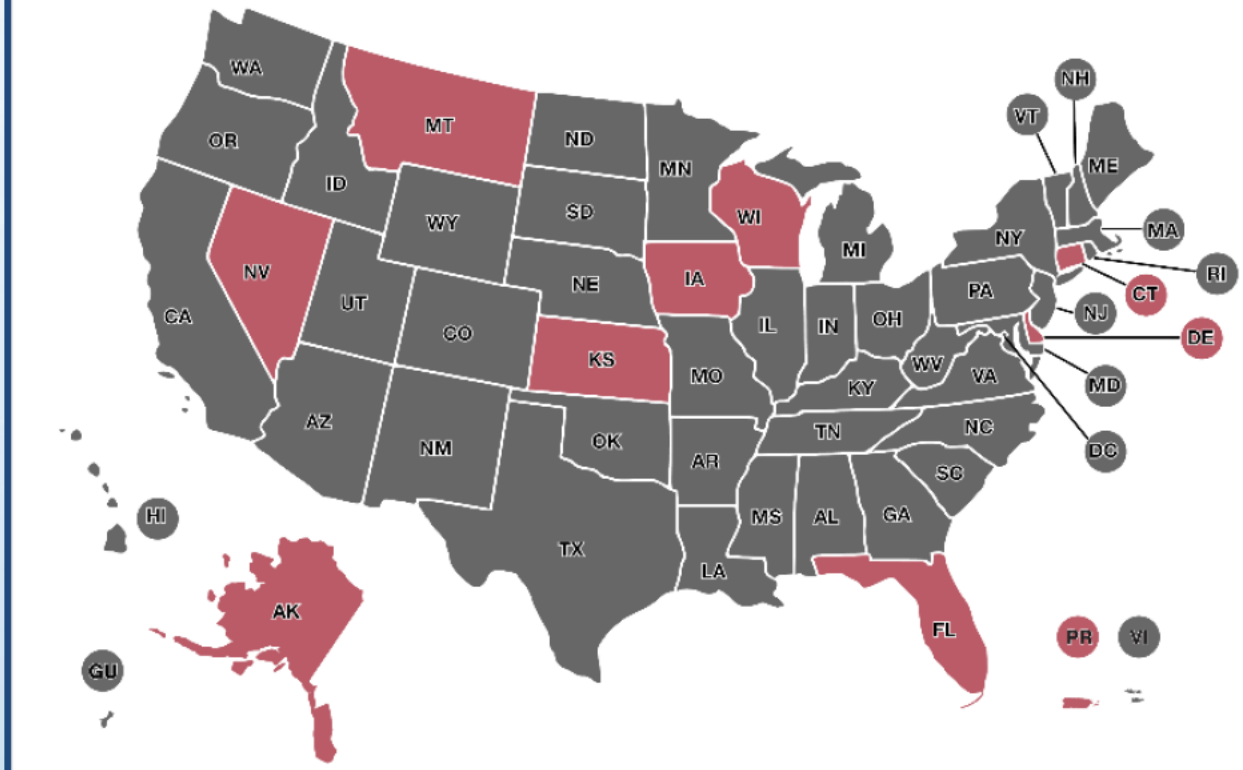
Message Keys: **Corrections Information Query (PCQ)**

Database accessible to Nlets users



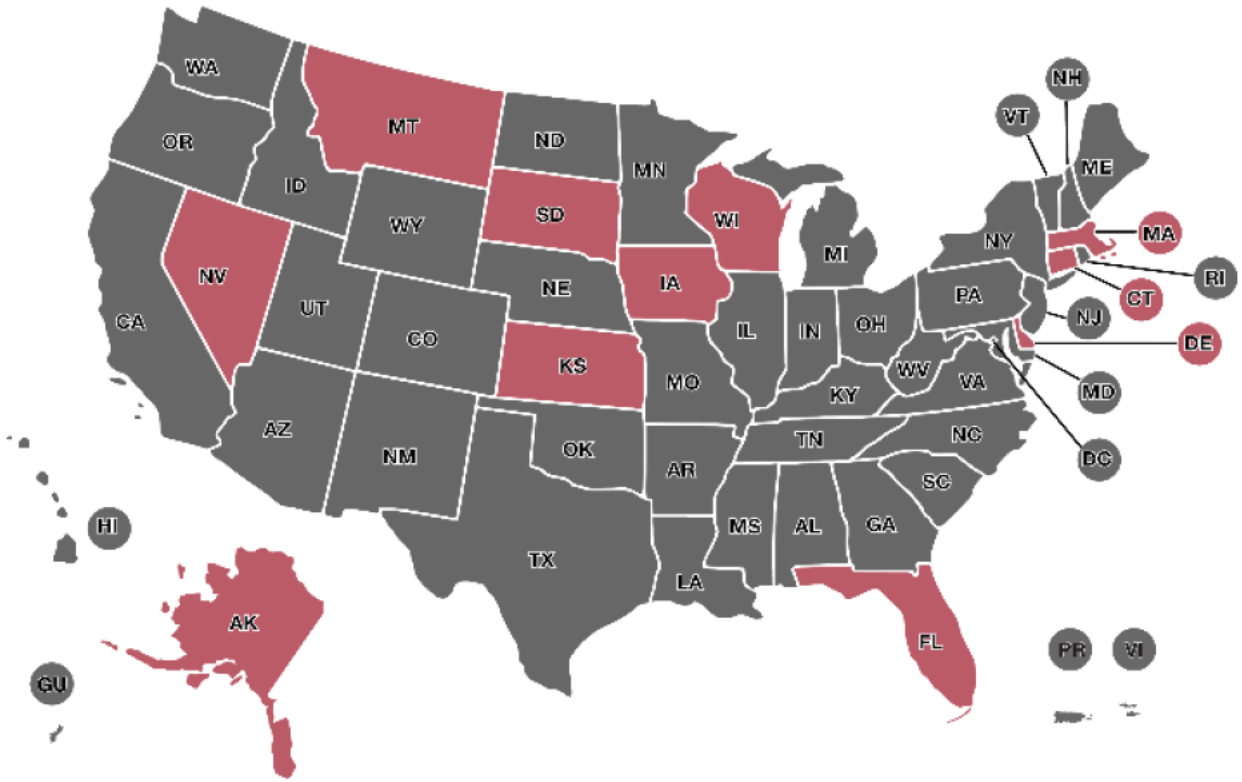
Message Keys: **Probation Query (PBQ)**

Database accessible to Nlets users



Message Keys: **Parole Query (PPQ)**

Database accessible to Nlets users





Section 36 Nlets WIKI

International Fuel Tax Association (IFTA)

Powered By Nlets

The purpose of the International Fuel Tax Association transaction is to identify companies severely delinquent in paying their fuel taxes.





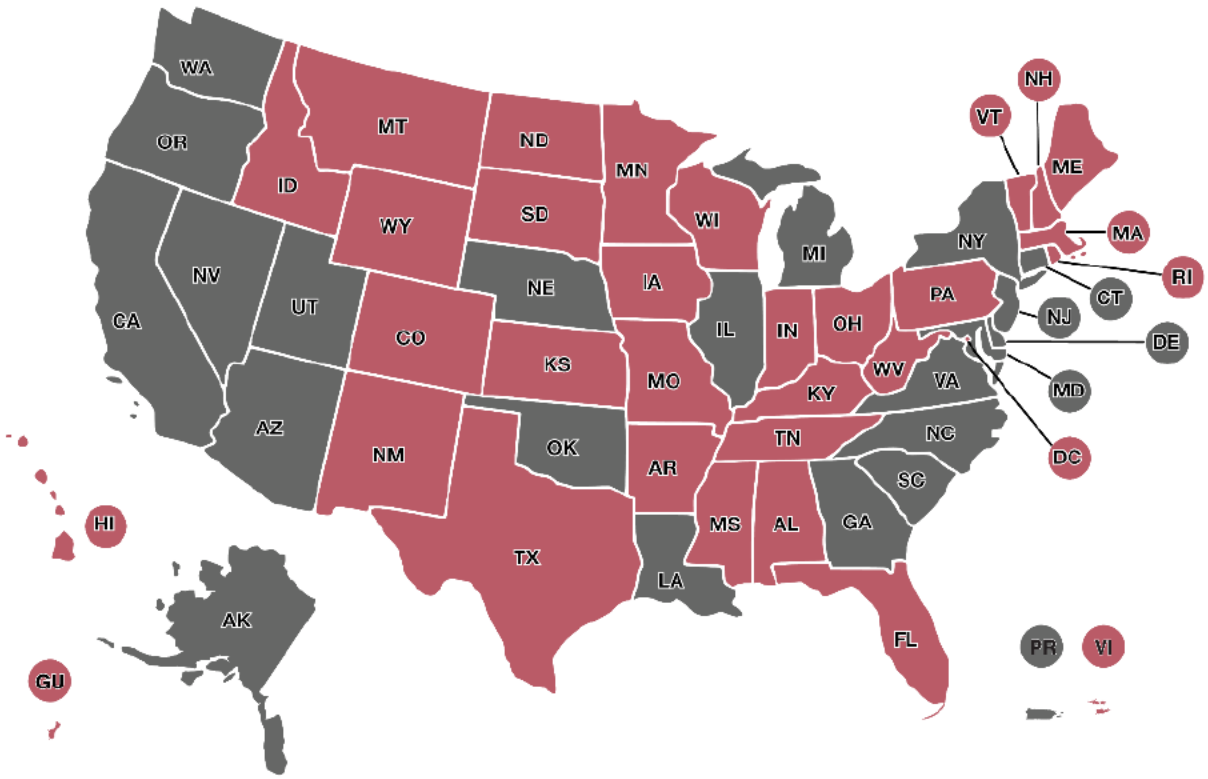


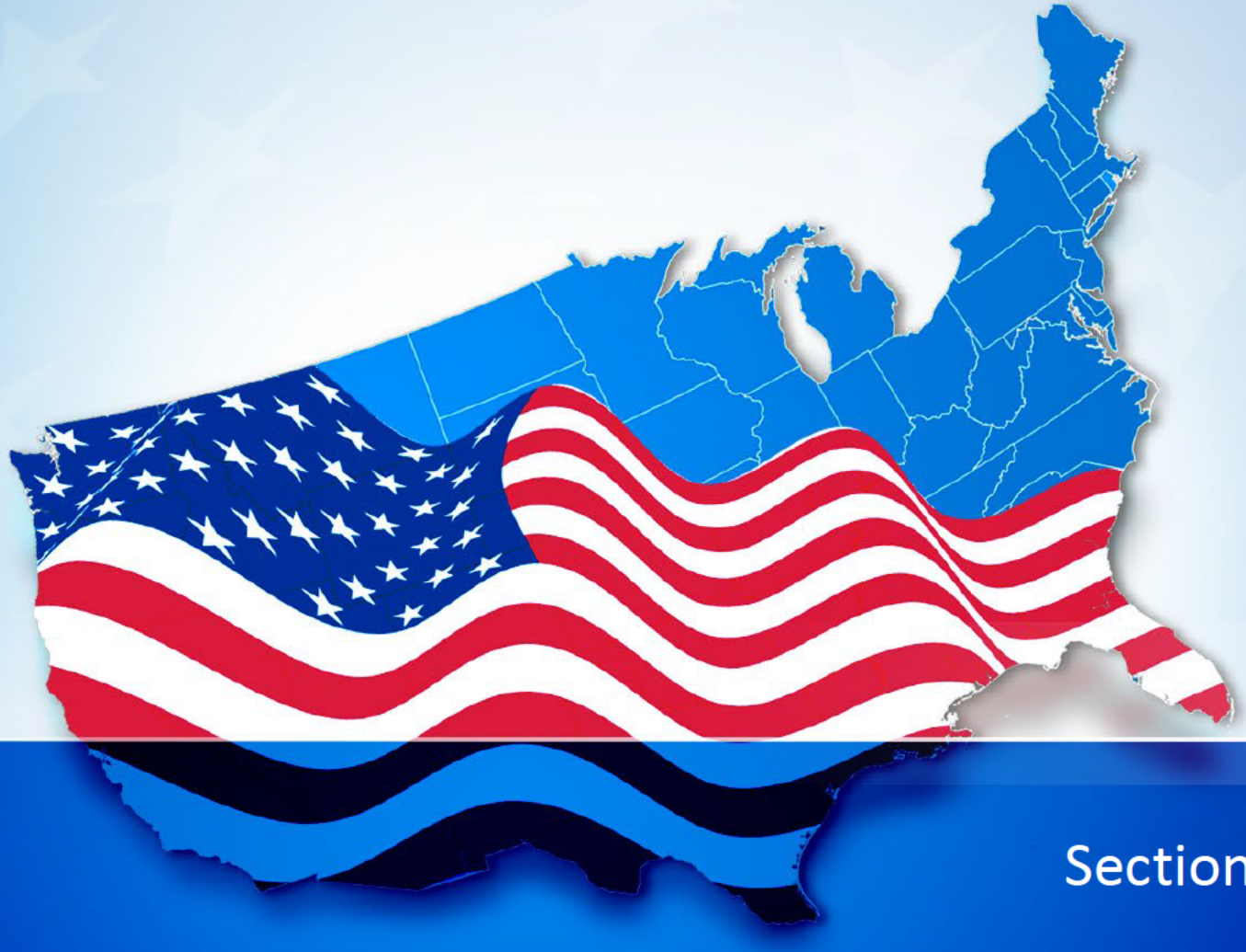
There are only two types of agencies that can access the IFTA file:

- Those agencies charged with the ***enforcement of fuel tax laws*** within a state or province
- Law enforcement or criminal justice agencies for ***investigative purposes***

Message Keys: **IFTA Query (FCQ)**

Configured to Send this Query





Section 35 Nlets WIKI

INTERPOL

INTERPOL

CONNECTING POLICE FOR A SAFER WORLD

Powered By Nlets



Access to INTERPOL records via Nlets provides information on ***international wanted persons, stolen vehicles, and stolen travel documents.***





IPQ – Wanted Person Query

FPQ – Wanted Person Query – ***full record***

IVQ – Stolen Vehicle Query

FVQ – Stolen Vehicle Query – ***full record***

ITQ – Stolen Travel Document Query

FTQ – Stolen Travel Document Query – ***full record***



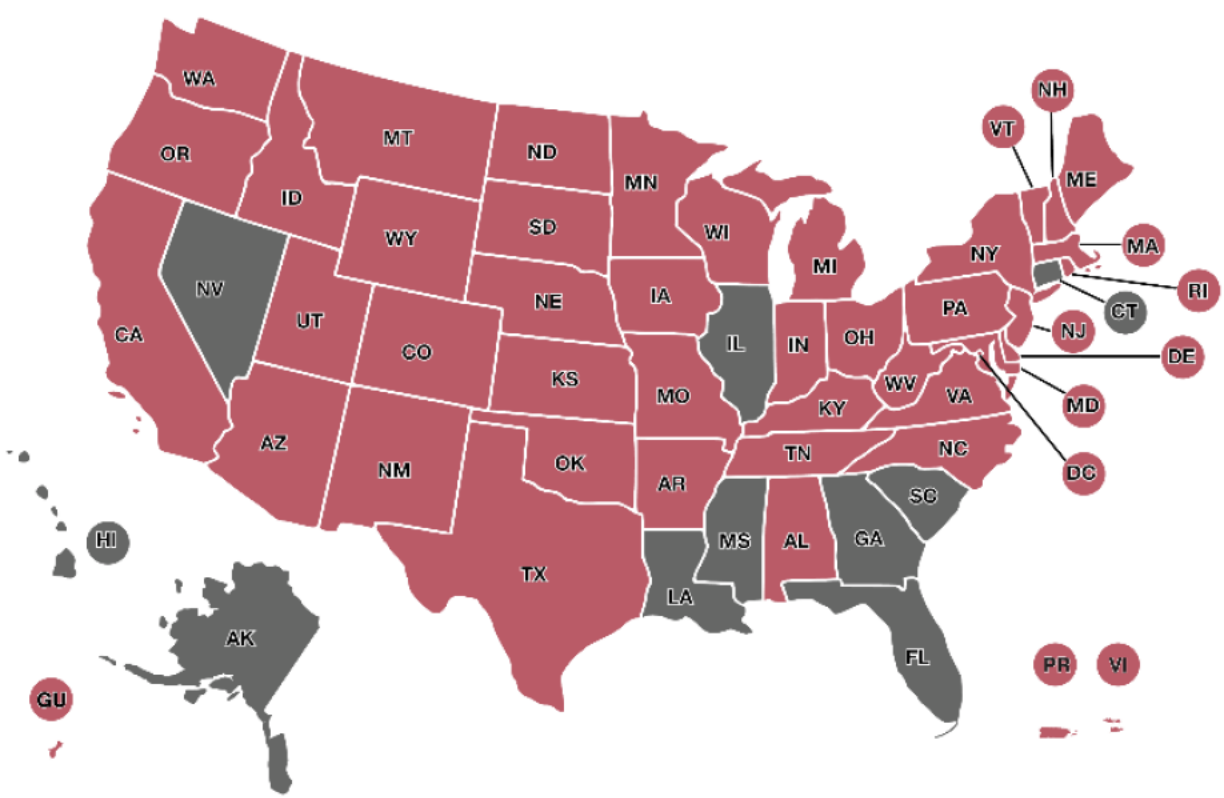


All queries to INTERPOL are sent to the two-character destinations of IP, which will result in a check of the international police database in Lyon, France.

190 participating countries!!

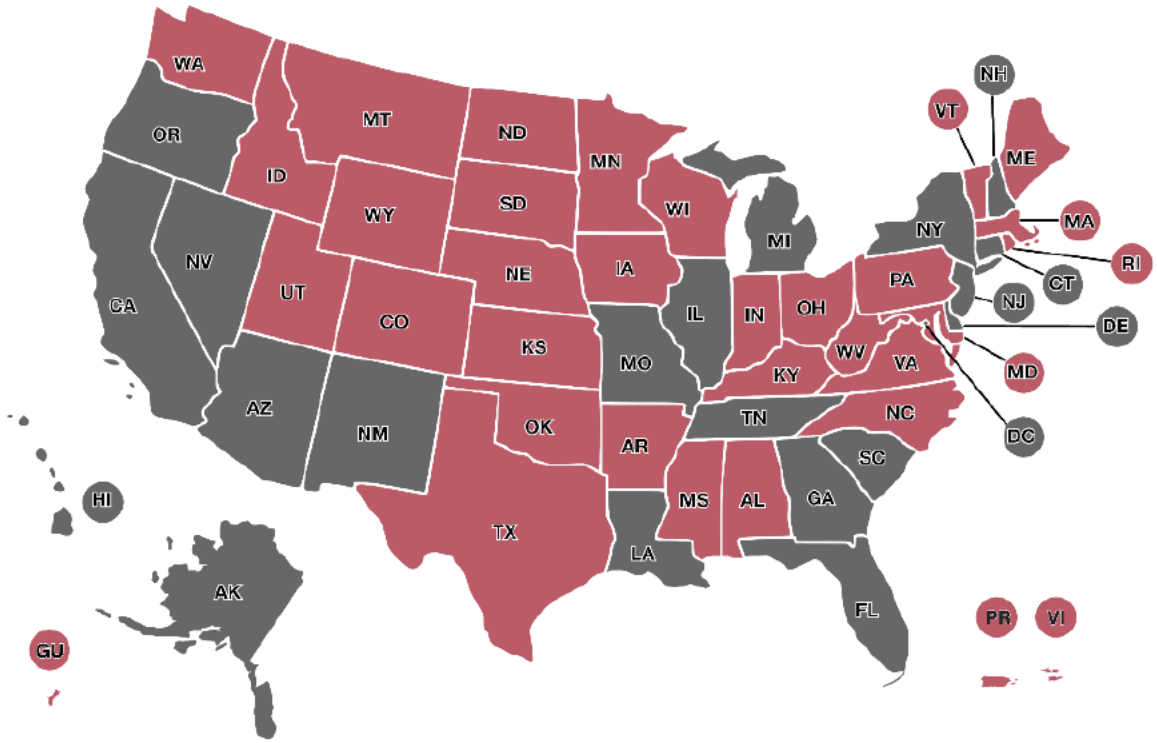
Message Keys: **INTERPOL Wanted Person Full Inquiry (FPQ)**

Configured to Send this Query



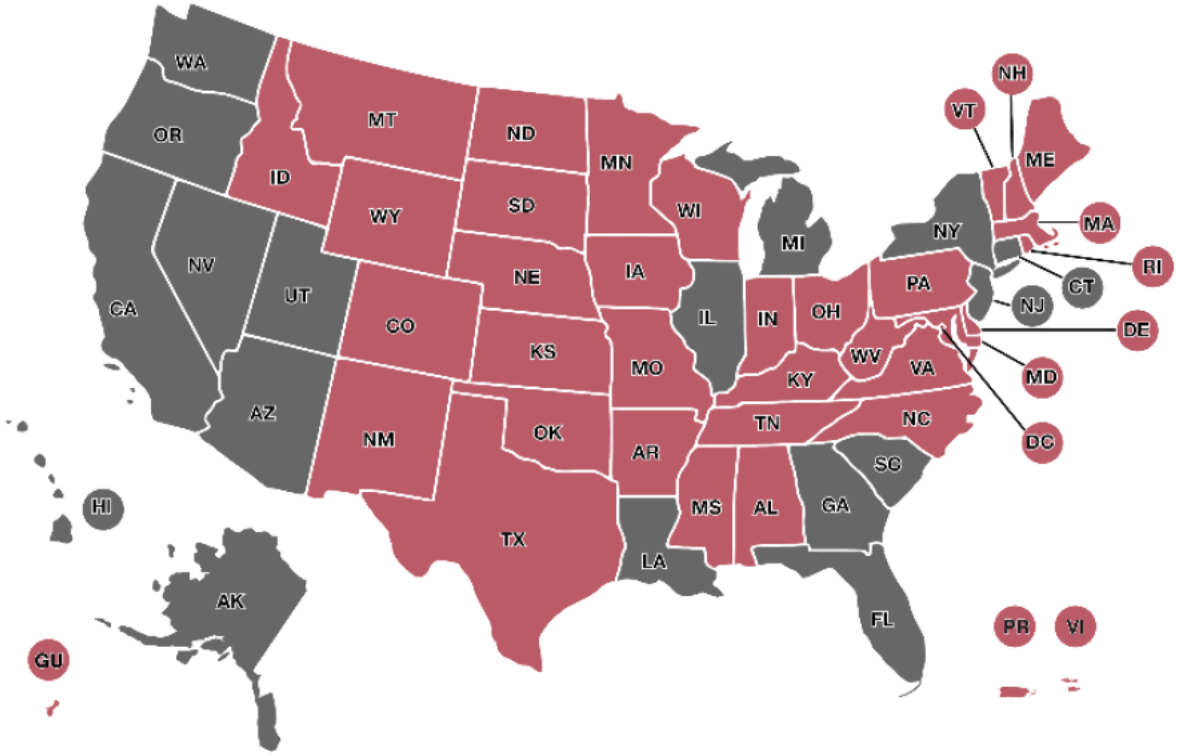
Message Keys: **INTERPOL Stolen Vehicle Full Query (FVQ)**

Configured to Send this Query



Message Keys: **INTERPOL Stolen Travel Document Full Query (FTQ)**

Configured to Send this Query





Section 35 Nlets WIKI

INTERPOL Gun Query

INTERPOL

CONNECTING POLICE FOR A SAFER WORLD

Powered By Nlets

The IGQ message key will access an INTERPOL web-based system called iARMS, which ***facilitates information exchange*** and cooperation between law enforcement agencies on ***firearms crime.***





iARMS can be functionally divided into three modules:

- Firearm Records Module
- *Trace Request Module *not available
- *Statistics and Reports Module *not available

What is the Firearm Records Module?

It enables authorized law enforcement officers to:

- Create, manage, and share records of lost, stolen, trafficked, or smuggled firearms;
- Notify a country when a recorded firearm is seized;
- Generate reports on lost, stolen, trafficked, or smuggled firearms



Specifications were modeled after the NCIC stolen gun check (QC)

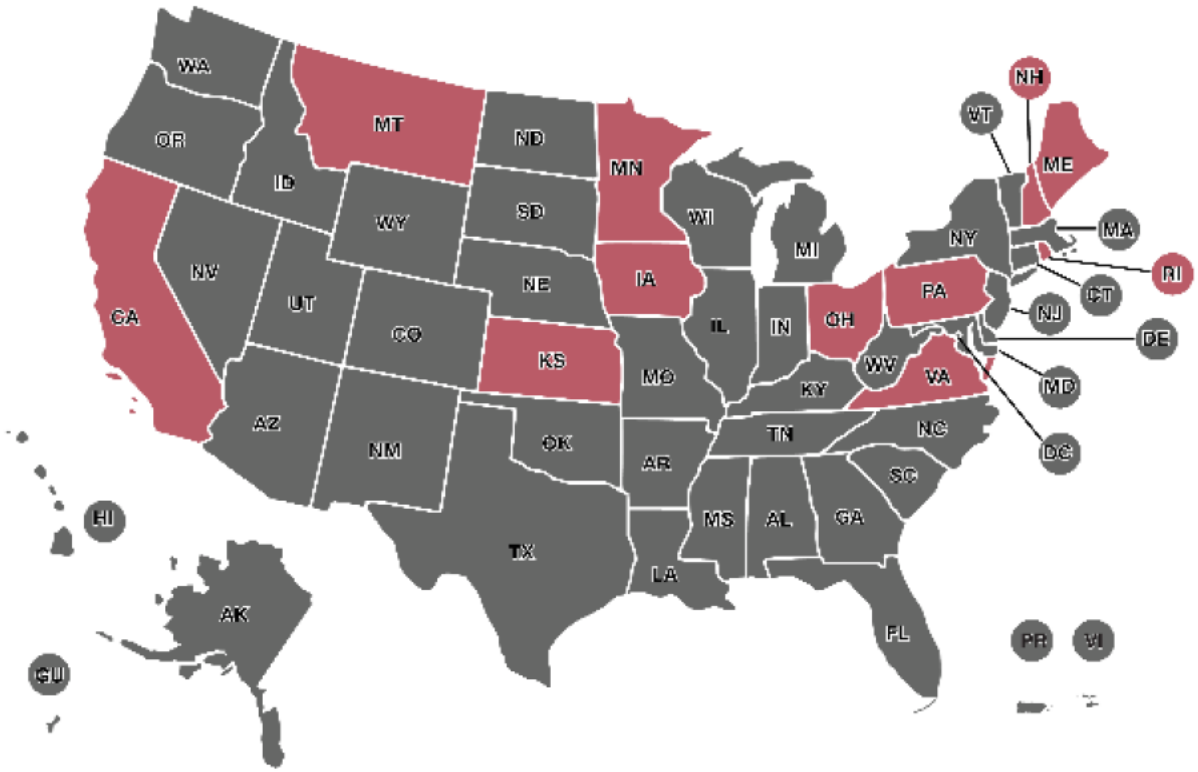
Query by ***serial number*** or ***INTERPOL record ID***

Can be federated at the state level



Message Keys: **INTERPOL Gun Query (IGQ)**

Configured to send this query





Section 42 Nlets WIKI

Law Enforcement Information Sharing Service

Powered By Nlets

Facilitates the sharing of information from Immigration and Customs Enforcement (ICE) databases with federal, state, and local law enforcement agencies.





This transaction (GPQ) searches the ICEPIC database for subject to return ***complete biographic and biometric data.***

Biographical data includes names, aliases, date of birth, phone numbers, addresses, nationality

Biometric data include fingerprints and photographs.



The information may be used for the following purposes:

- Assist with investigations
- Notify officials of past criminal behavior
- Validate person of interests key biographic and biometric information

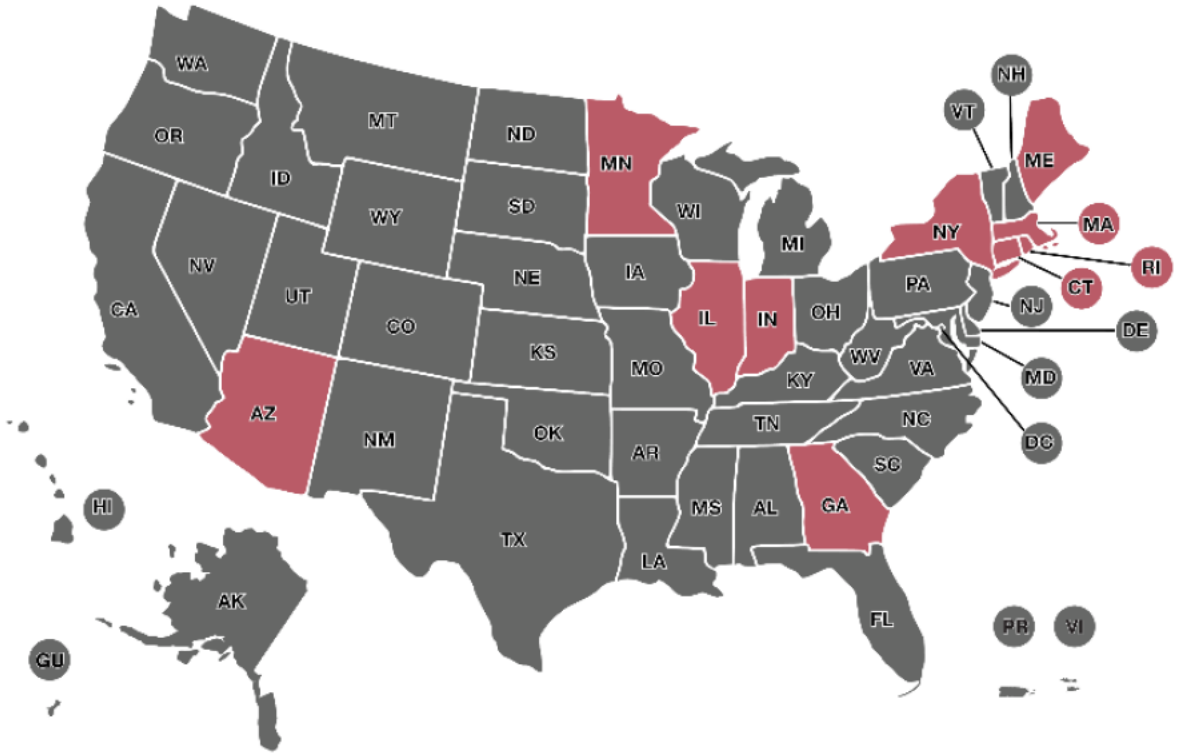


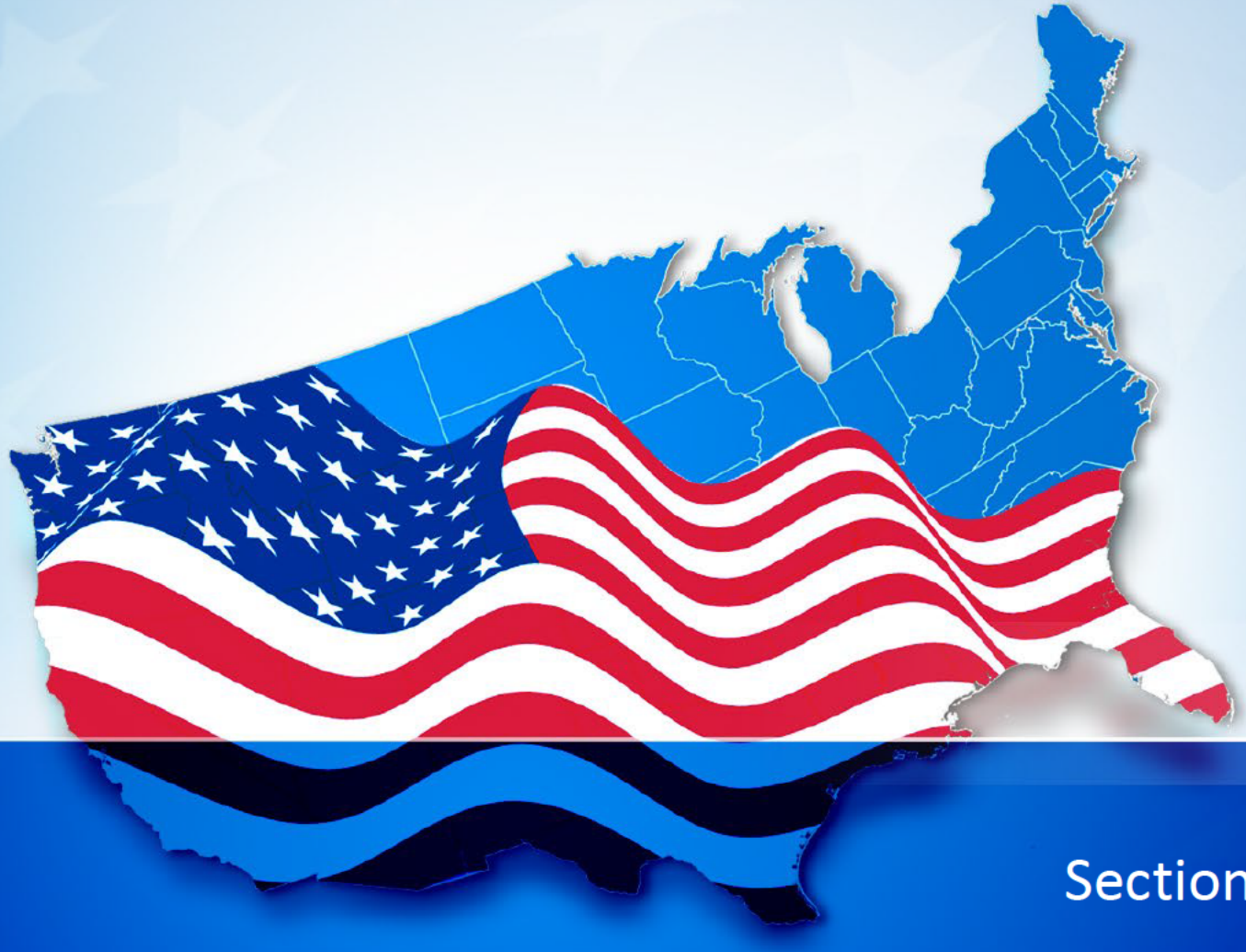
Response data includes information provided by individuals when ***applying for U.S. immigration benefits / admission into the U.S.***

In some situations the information comes from DHS enforcement encounters.

Message Keys: **General Person Query/LEISS (GPQ)**

Configured to Send this Query





Section 19 Nlets WIKI

Immigration Alien Transactions

Powered By Nlets

The purpose of this transaction is to provide timely information on ***aliens suspected of criminal activity*** and ***status information of aliens under arrest.***



The IAQ will search 13 ICE databases in addition to NCIC and III.



The response comes from the Law Enforcement Support Center (LESC) staff.



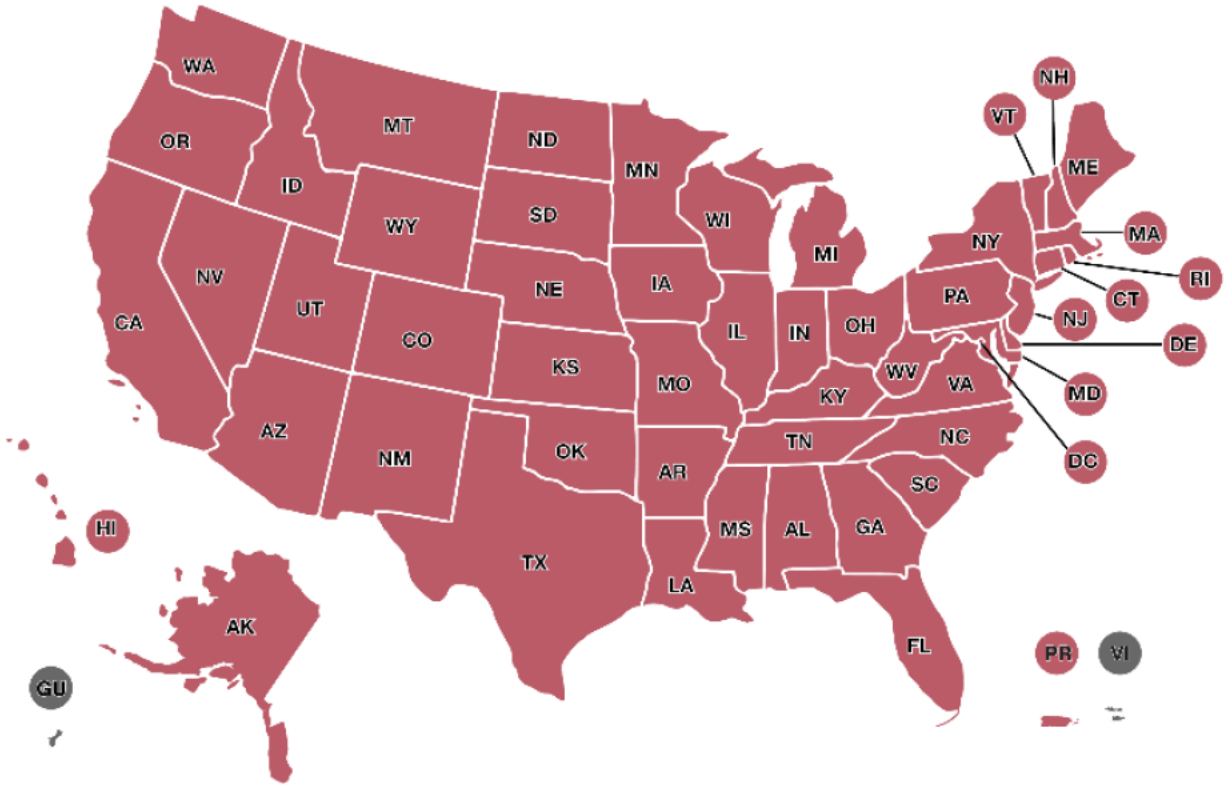
The information you get from these databases can be used:

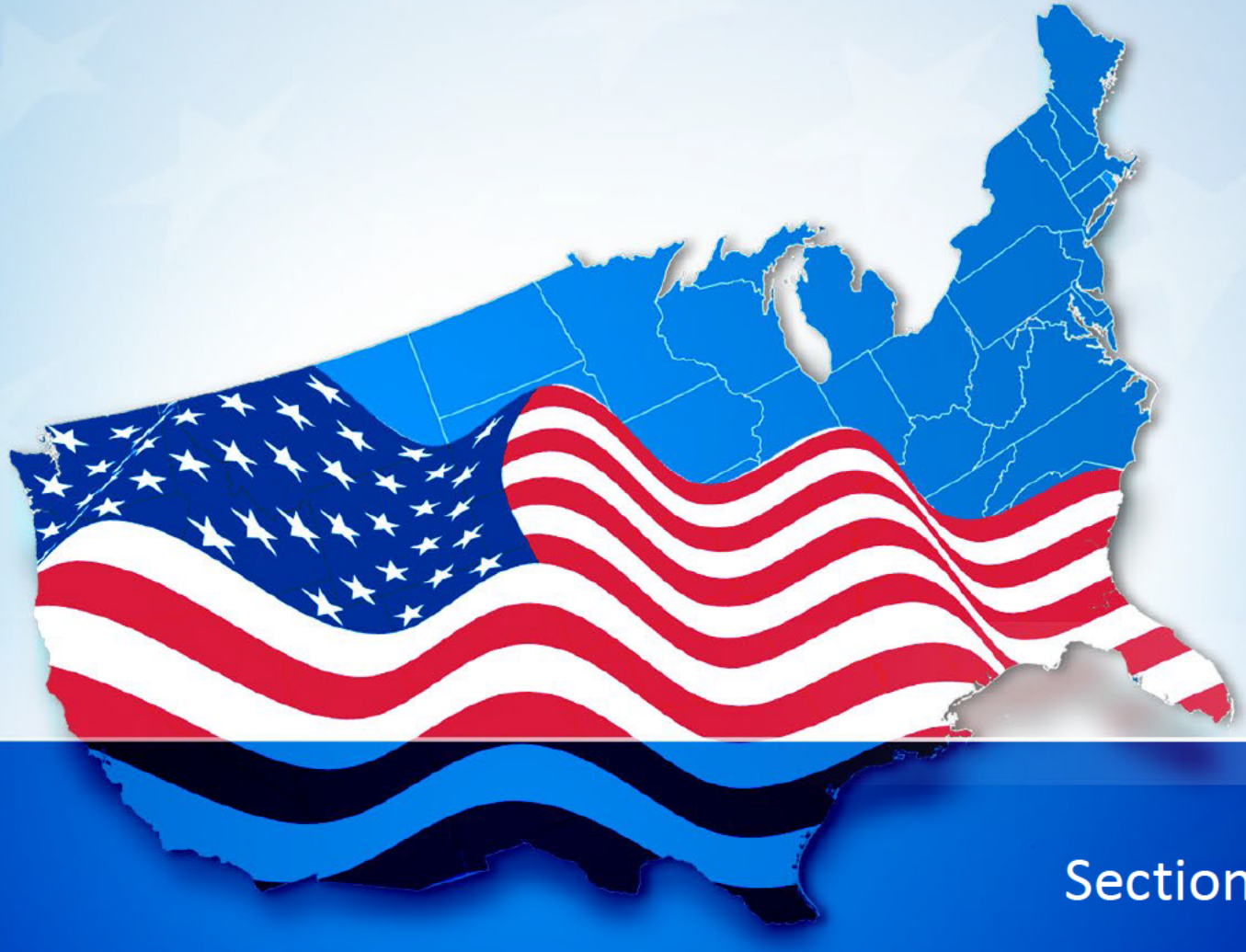
- To assist with ***investigations***
- To ***provide identification and background information*** on subjects for correctional departments
- To ***notify ICE*** of a subjects incarceration or placement on probation.



Message Keys: **Immigration Alien LESC Query (IAQ)**

Configured to Send this Query





Section 28 Nlets WIKI

License Plate Reader

Powered By Nlets



The purpose of this national license plate reader sharing program was to ***create a consolidated LPR repository across the U.S.*** to search and locate LPR data.



The initial source of LPR data is the states/federal agencies that maintain their own LPR repositories.





This will enable the authorized community of Nlets to determine if any other contributing law enforcement agency has captured a vehicle's license plate of interest.



Separate from the national LPR pointer index, there are three other transactions you can run to obtain LRP data:

- RQ to VS (National Vehicle Service)
- RQ to NA (National Insurance Crime Bureau)
- RQ to LP (Combination of Both

RQ to VS (National Vehicle Service)

Access to a central repository populated by:

- Towing companies
- Repossession companies
- Parking lots
- Garages
- Toll way systems



Query by license plate number and license plate year

*Note – NVS also proactively compares their database to the NCIC stolen vehicle file

RQ to NA (National Insurance Crime Bureau)

LPRs were initially installed by CBP to develop and track movement of vehicles as they crossed through ports of entry:

- SW border between the U.S. and Mexico
- Northern border between the U.S. and Canada

CBP provides NICB raw LPR data as a toll in its efforts to prevent and investigate vehicle theft and insurance fraud.

Query by license plate number and license plate year

RQ to LP (Access to both NVS and NICB)



Information from ***both*** NVS and CBP (via NICB) can be obtained through a single vehicle registration transaction (RQ) to destination 'LP'

IACP LPR Website

http://ww[illegible]p.org/ALPR





DAILY NEWS

World - Business - Finance - Lifestyle - Travel - Sport - Weather

Issue: 240104 THE WORLDS BEST SELLING NATIONAL NEWSPAPER Est - 1965

HARDY, Va. --Virginia State Police found suspected gunman Vester L. Flanagan II using a license plate reader.

An almost five-hour manhunt had ensued after authorities said Flanagan gunned down a Virginia reporter and cameraman for WDBJ on live television Wednesday, August 26.

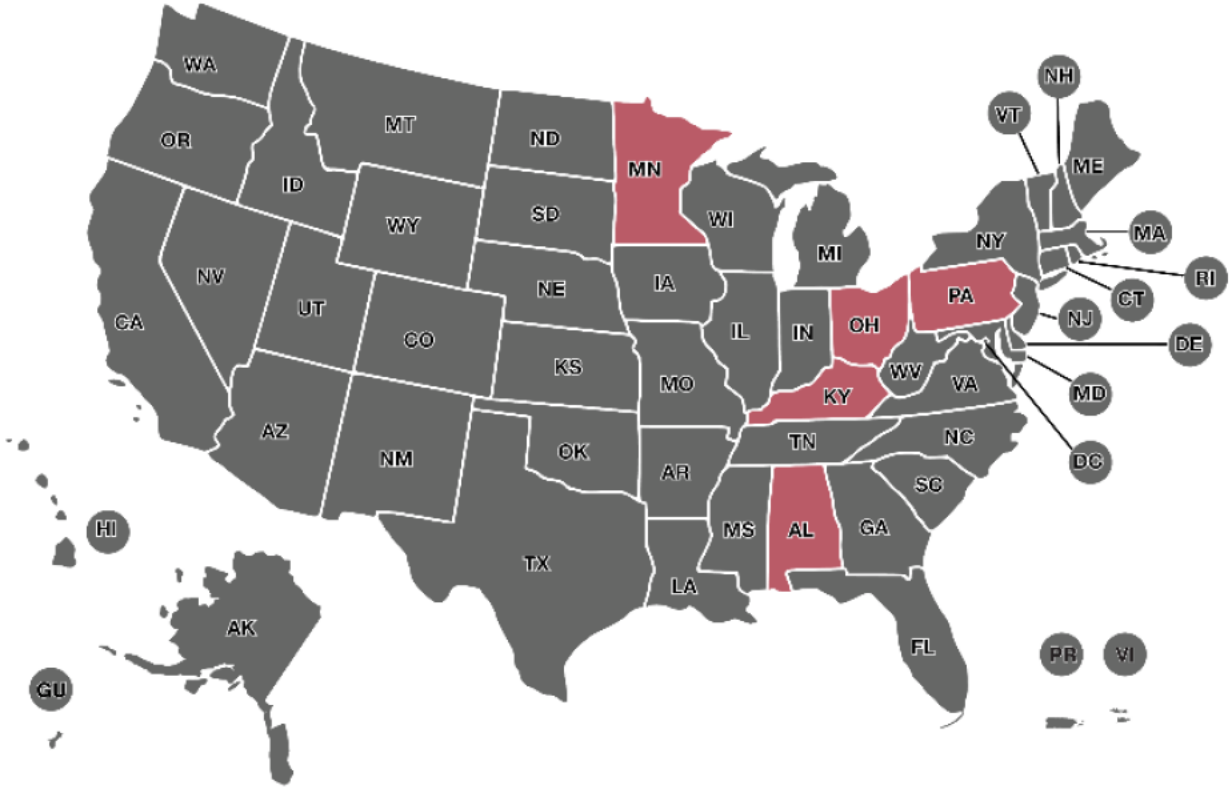
The two young lives lost from Roanoke, Virginia worked for sister station WDBJ. They were 24-year-old Alison Parker and 27-year-old Adam Ward. Chamber of Commerce Executive Director Vicki Gardner was wounded in the shooting and is in stable condition.

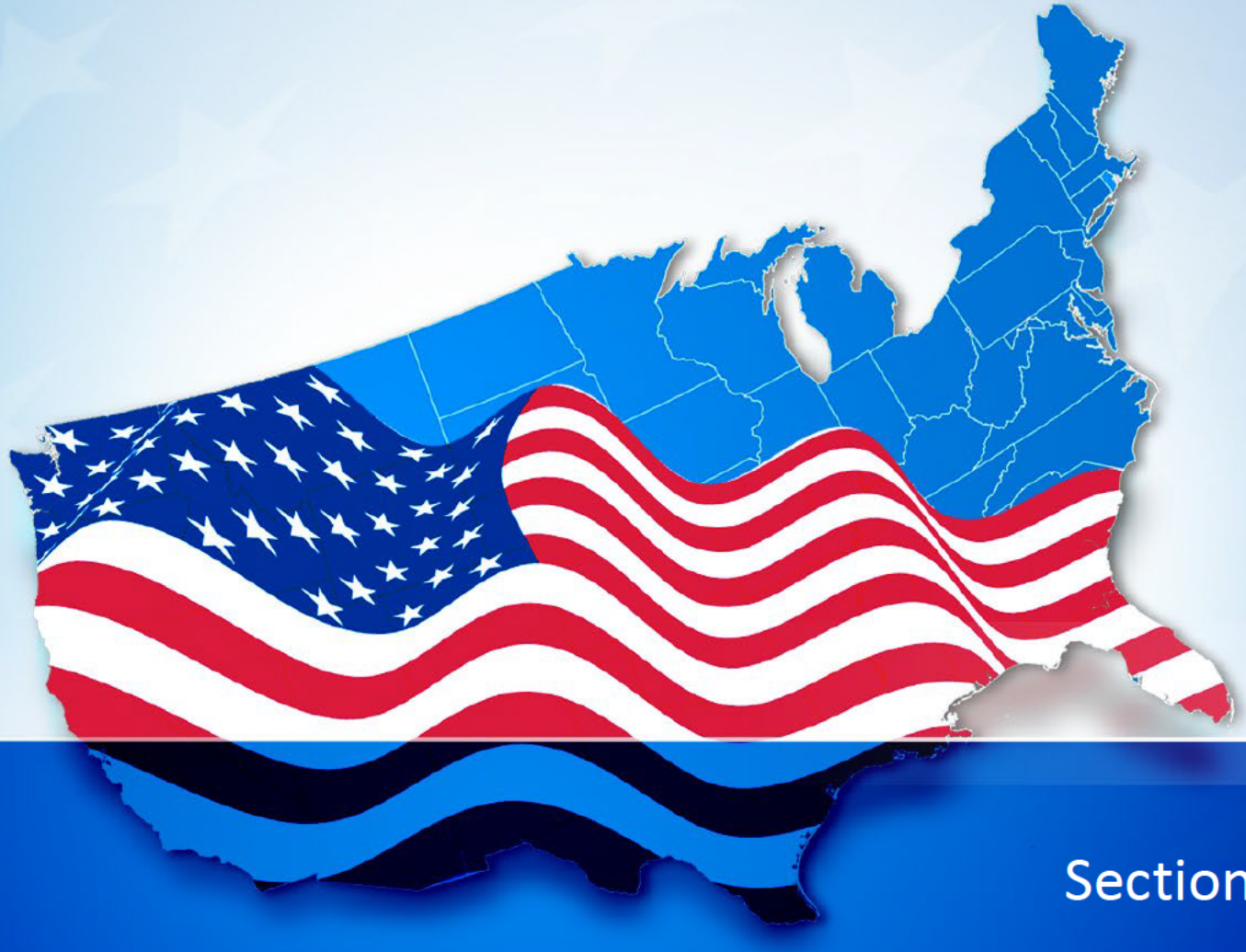
Flanagan, who previously reported at WDBJ -- known on-air as "Bryce Williams" -- fled from the scene and was found hours later on Interstate 66 in Faquier County.

At a press conference Sgt. Rick Garletts, with VSP, said that Trooper Pam Neff, was on patrol along I-66.

Message Keys: **License Plate Reader Query (LPQ)**

Configured to Send this Query





Section 26 Nlets WIKI

Commercial Vehicle Information

Powered By Nlets

User's can send:

- Driver License Query (DQ)
- Driver History Query (KQ)
- Registration Query (RQ)

Destination:

- MX

The appropriate Mexican commercial driver data will be returned.





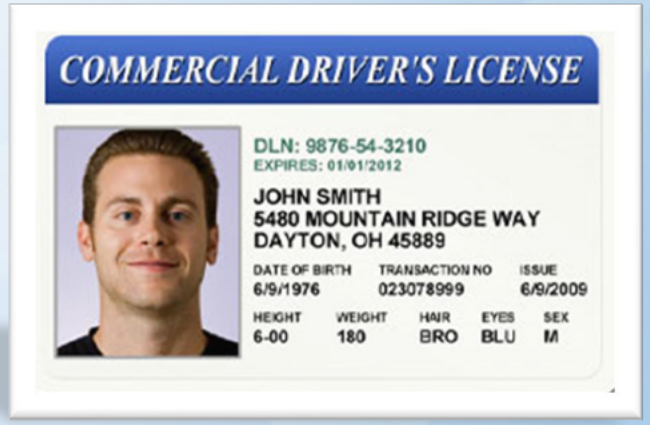
U.S. Commercial Driver License Data Now Available Through Nlets!

User's can send:

- Driver License Query (DQ)
  - Must include license state (OLS)
- Driver History Query (KQ)

Destination:

- CL



The appropriate U.S commercial driver data, ***including medical certifications***, will be returned in real-time.



PRISM

Performance and Registration Information System Management File



The PRISM system provides Nlets users with access to ***safety information on motor carriers and the vehicles*** that are assigned to those motor carriers.



Carrier status queries ***to PRISM*** use the two-character destination code “FM” using message key ‘ACQ’

Carrier status queries ***to SaferSys*** use the two-character destination code ‘CL’ also using message key ‘ACQ’

The PRISM system also provides Nlets users with access to ***vehicle information***.



Vehicle information may be requested by:

- VIN
- License plate number and state



A message providing an overall assessment of the carrier's ***safety status*** will appear at the top of the response.

*Note that the PRISM system is now updated in real-time!



Please refer to the Nlets WIKI for a list of the Out of Service Orders (OOSO) that could potentially appear in the response.



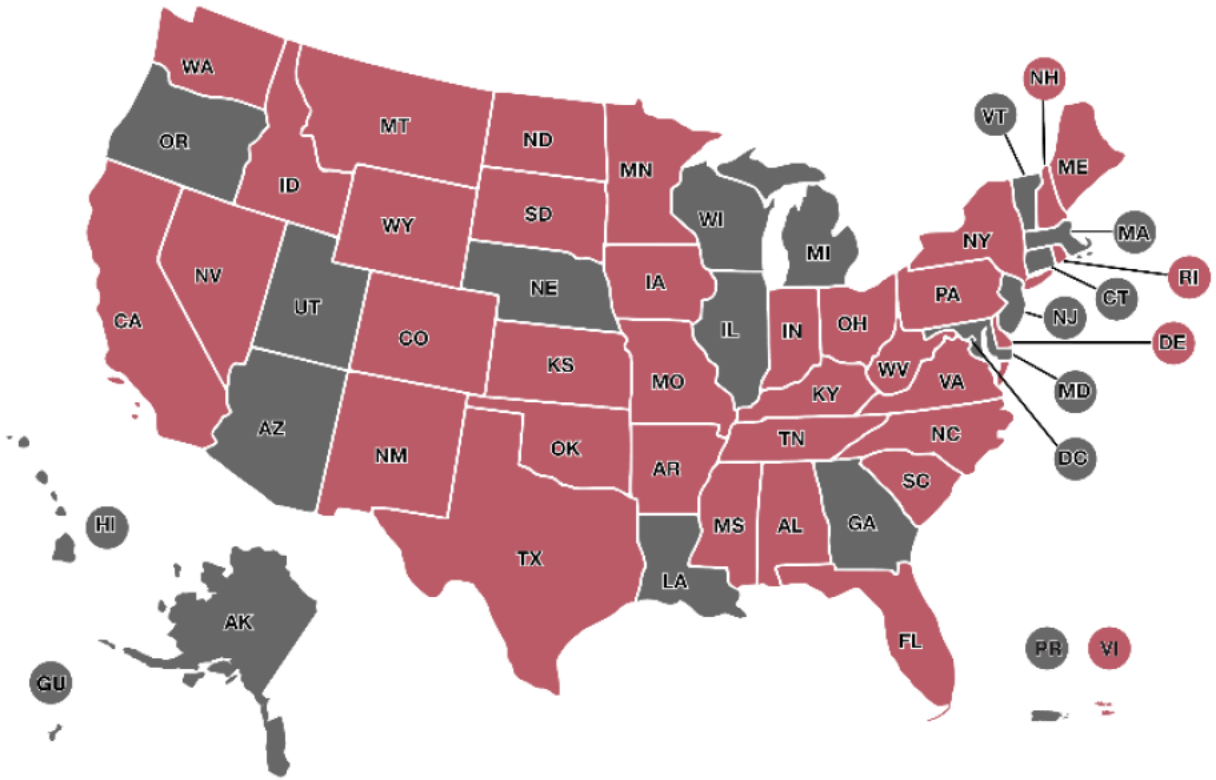
SaferSys

In 2012 Nlets added the additional capability to query ***licensing and insurance data*** contained in the vehicle search through a web scrape service.



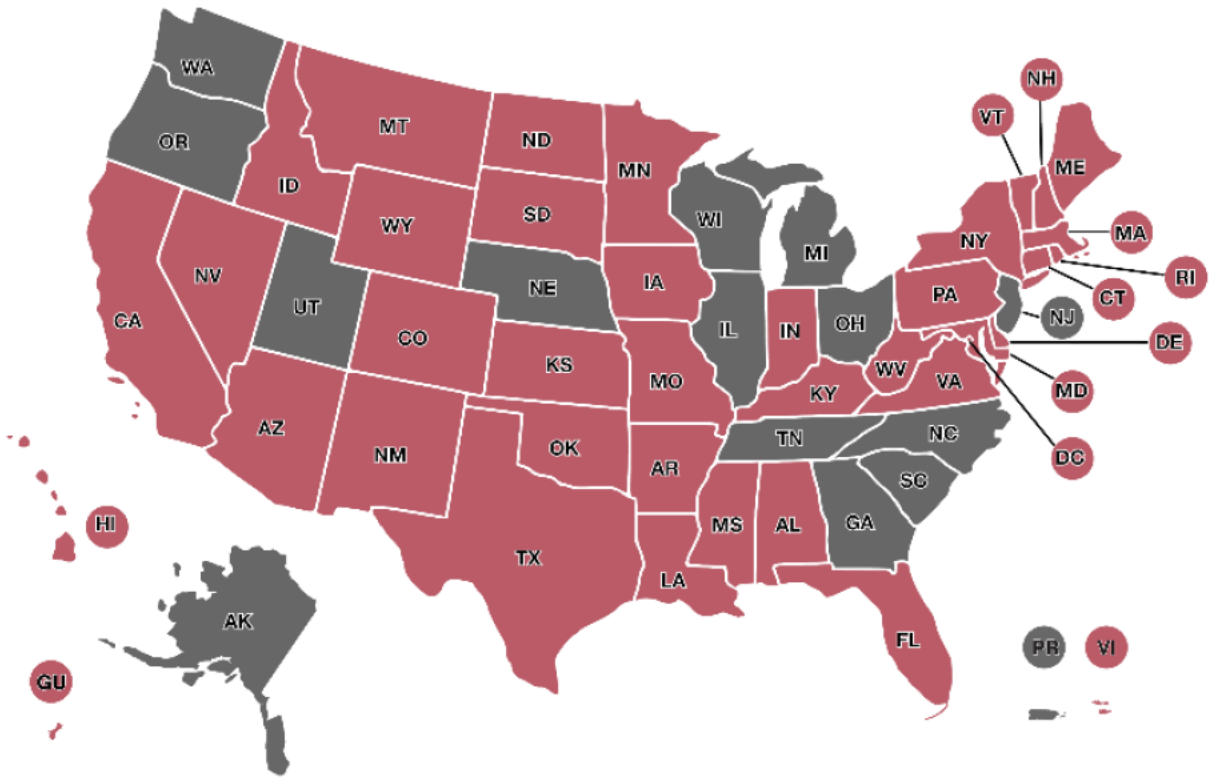
Message Keys: **Commercial Vehicle Carrier Status Query (ACQ)**

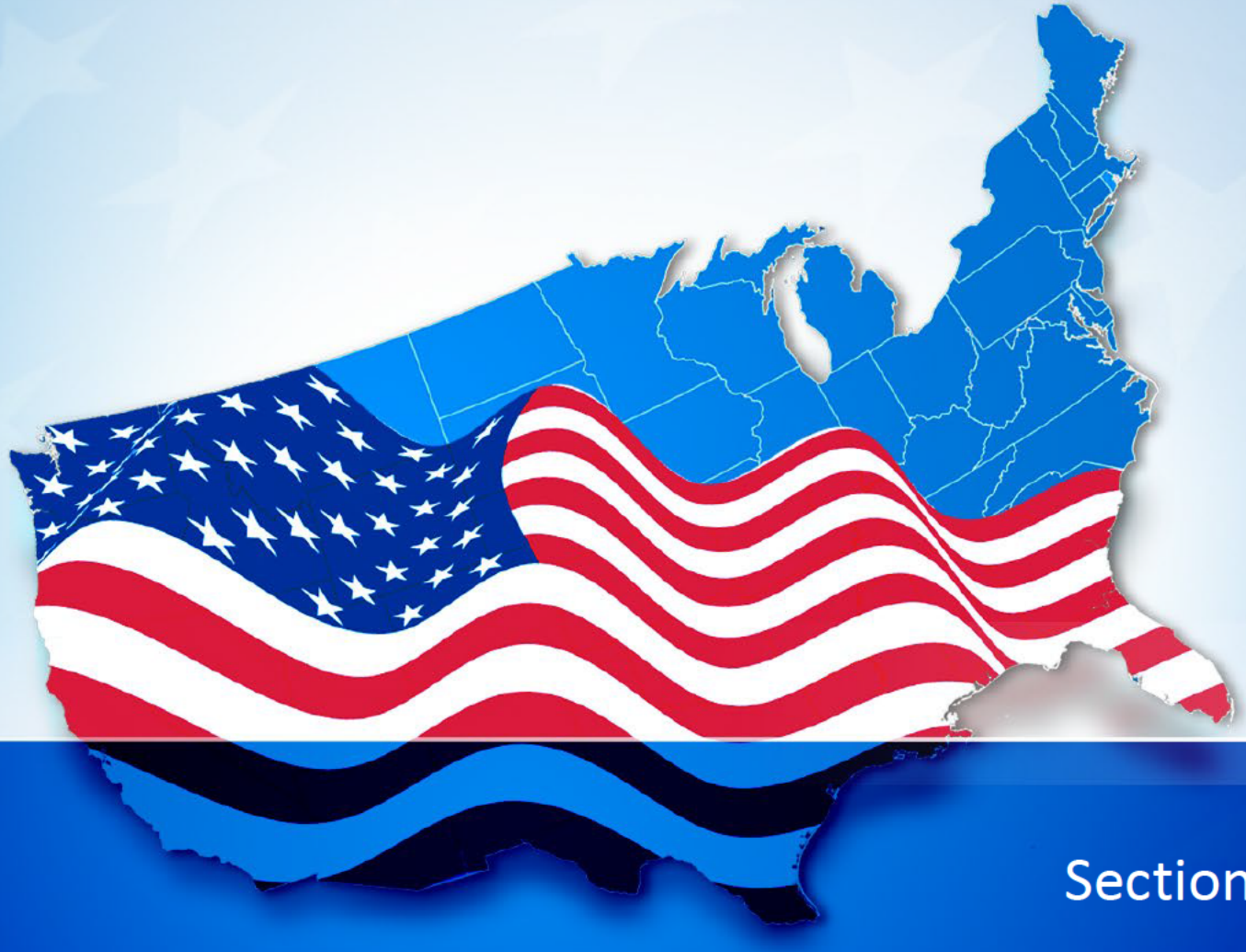
Configured to Send this Query



Message Keys: **Commercial Vehicle Status Query (AVQ)**

Configured to Send this Query





Section 27 Nlets WIKI

National Insurance Crime Bureau (NICB)

Powered By Nlets



The National Insurance Crime Bureau is a ***crime prevention organization assisting law enforcement*** in the prevention, detection, and prosecution of the financial crimes of theft, fraud, and arson relating to personal property.

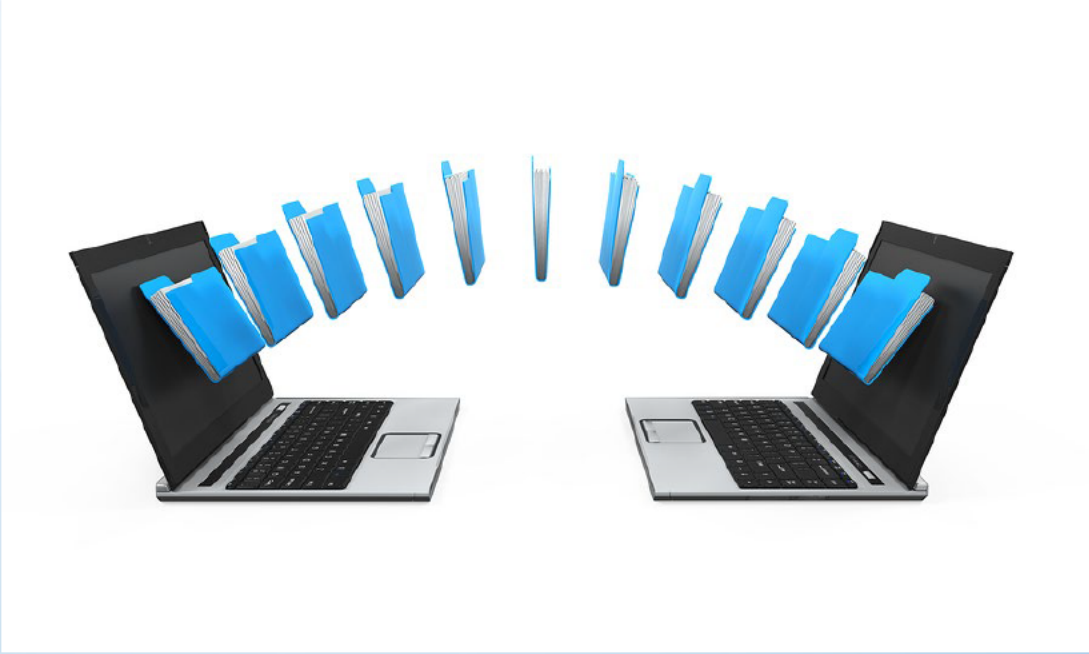
250 million records related to vehicles!





Stolen Vehicle Entries

Every stolen vehicle entered into NCIC will be passed to NICB by NCIC.



NICB will enter this record in their file and will ***cross-check the record against the 60 days of entries*** into the Impound, Export, Auctions, and International Index files.



If a match is made, the following message will be forwarded via Nlets to the entering agency:

THIS IS TO NOTIFY YOU THAT THE VEHICLE YOU ENTERED INTO NCIC, VIN/12345671234567890, IS IN THE NICB DATABASE. BELOW IS THE NICB RELATED VEHICLE RECORD. THIS MAY ASSIST YOU WITH ANY FOLLOW UP INVESTIGATION.
(followed by matching NICB record)

Impound file	Pre-Inspection File
Export File	Vehicle Claim File
Manufacturer's Shipping File	Rental File
Salvage File	Theft File
International Index File	Theft (recovery) File
Auction File	NCIC/CPIC Canceled File

NICB provides automated access to twelve different files via Nlets.

NIQ = Access to only the Impound and Export files

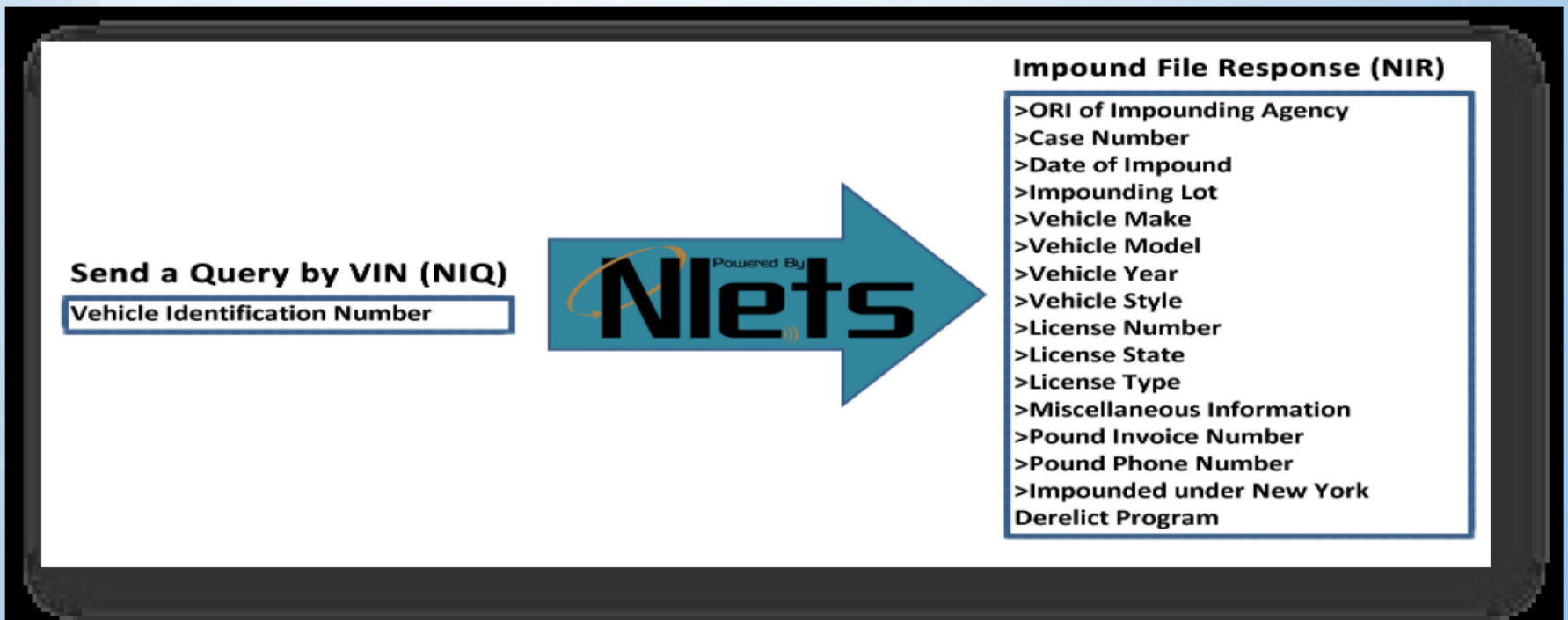
NAQ = Access to the other ten files

Impound File Query (NIQ)

Impound records will be returned ***only*** if the date of the impound is less than 60 days from the date of the inquiry.



Impound responses indicate that the vehicle has been impounded, but ***does not*** tell whether or not the vehicle was claimed or remains on the lot.





Export File Query (NIQ)

An export file response indicates that a vehicle has been exported out of the country, but it ***does not*** indicate if the vehicle has been returned to the country.





All Files Query (NAQ)



This transaction checks all available NICB, NVS, and OCRA (Mexican stolen) files with ***one exception***:

When a partial VIN search is requested, only the Manufacturer's Shipping file will be searched.

Shipping responses indicate to whom, when, and where a vehicle has been shipped.



Salvage responses indicate that the vehicle has been damaged, the cause of the loss, what the cash value was prior to the loss, the received value, and the appraised value.

Send a Query by VIN (NAQ)

Vehicle Identification Number

Powered By Nlets

Salvage File Responses

>Vehicle Year
>Vehicle Make
>Date of Salvage
>Cause of Claim/Loss
>Insurance Company
>Insurance Company Address
>Insurance Company Phone
>Claim Number
>Actual Cash Value
>Received Value
>Appraised Value



NICB maintains records of ***internationally stolen and salvaged*** vehicles from Canada, Germany, France, Sweden.



Send a Query by VIN (NAQ)

Vehicle Identification Number

Powered By Nlets

International Index Salvage Responses

>Vehicle Year, Make
>Date of Salvage
>Cause of Claim/Loss
>Insurance Company
>Insurance Company Address
>Insurance Company Phone Number
>Claim Number
>Actual Cash Value
>Received Value
>Appraised Value

Auction responses include those records that are processed through an auction house prior to the sale and sent to NICB.



Pre-inspection responses are returned on vehicles that are processed through an authorized pre-inspection center and do not pass processing through NICBs VINASSIST program.

Send a Query by VIN (NAQ)

Vehicle Identification Number

Powered By Nlets

Pre-Inspection File Responses

>Pre-Inspection Company
>Inspection Date
>Inspection Company File Number
>Odometer

Several rental car agencies provide and maintain a complete inventory on the NICB system.

When an ***impound*** or ***export is processed, it is automatically checked against this file.***

Send a Query by VIN (NAQ)

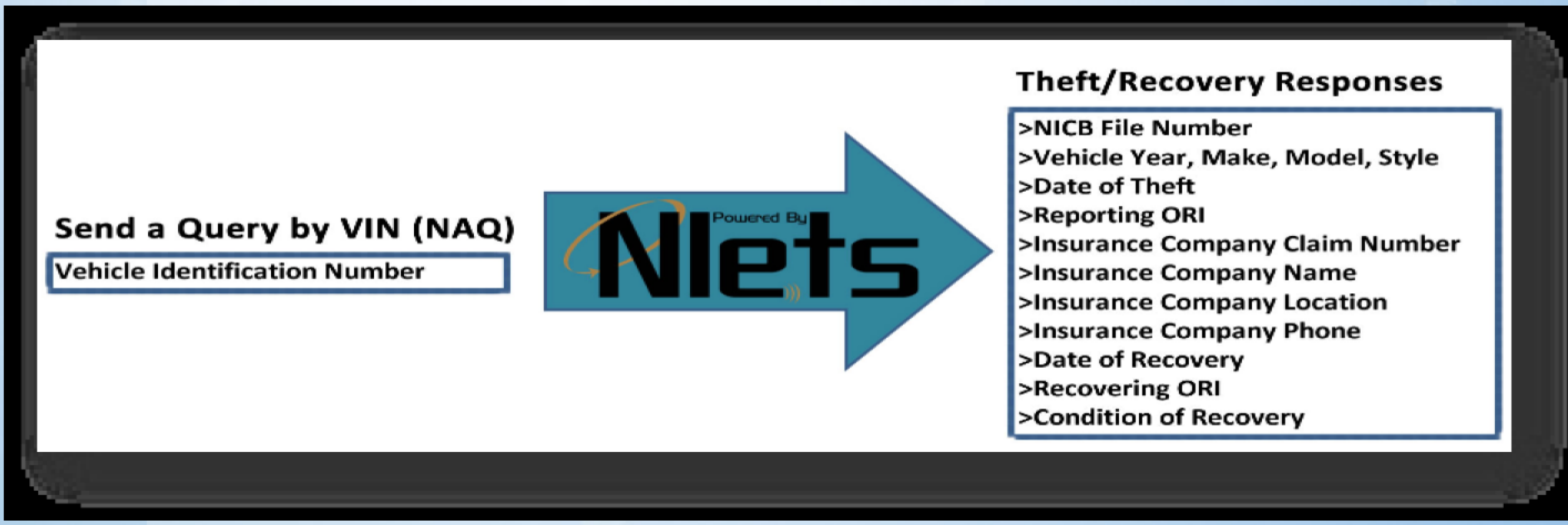
Vehicle Identification Number

Powered By Nlets

Rental File Responses

>Rental Company Name
>Rental Company File Number
>Date of Last Action on Vehicle
>Reason Vehicle is on File
>Name of Customer (Renter)

The ***recovery information mirrors the theft record*** except that the vehicle recovery information is also displayed.



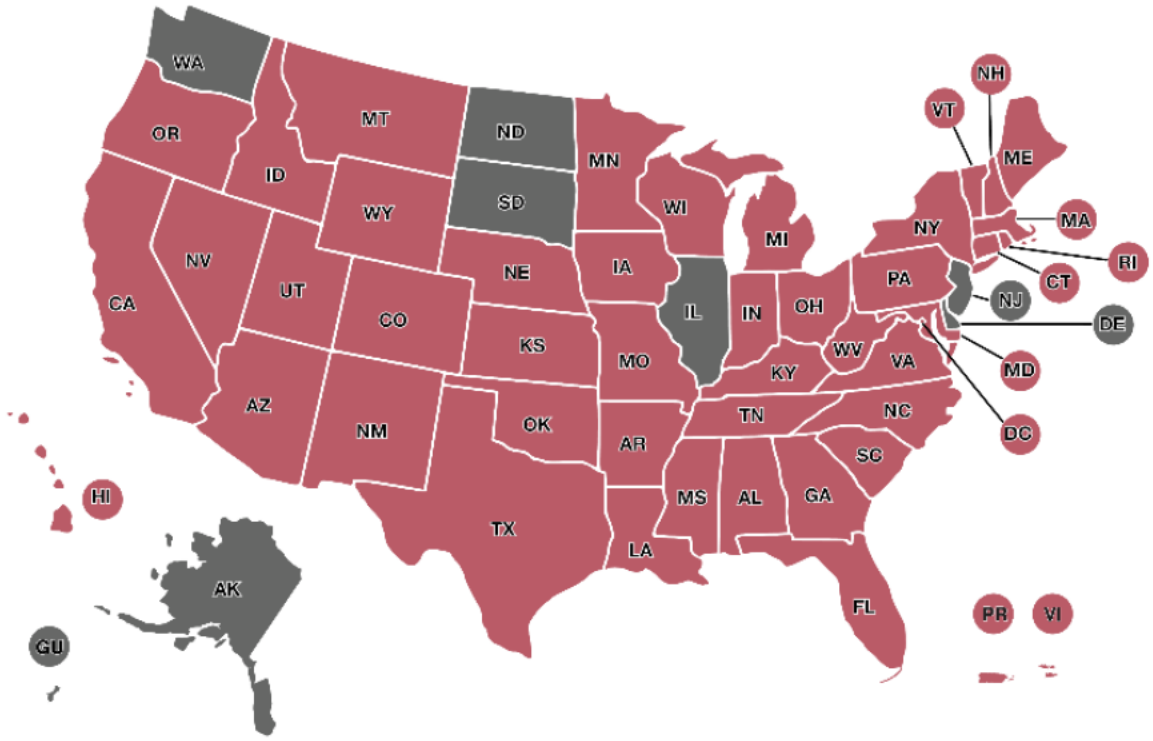
NICB maintains NCIC ***cancelled*** records online dating back to 1972.

NICB maintains CPIC ***cancelled*** records online dating back to 1996.



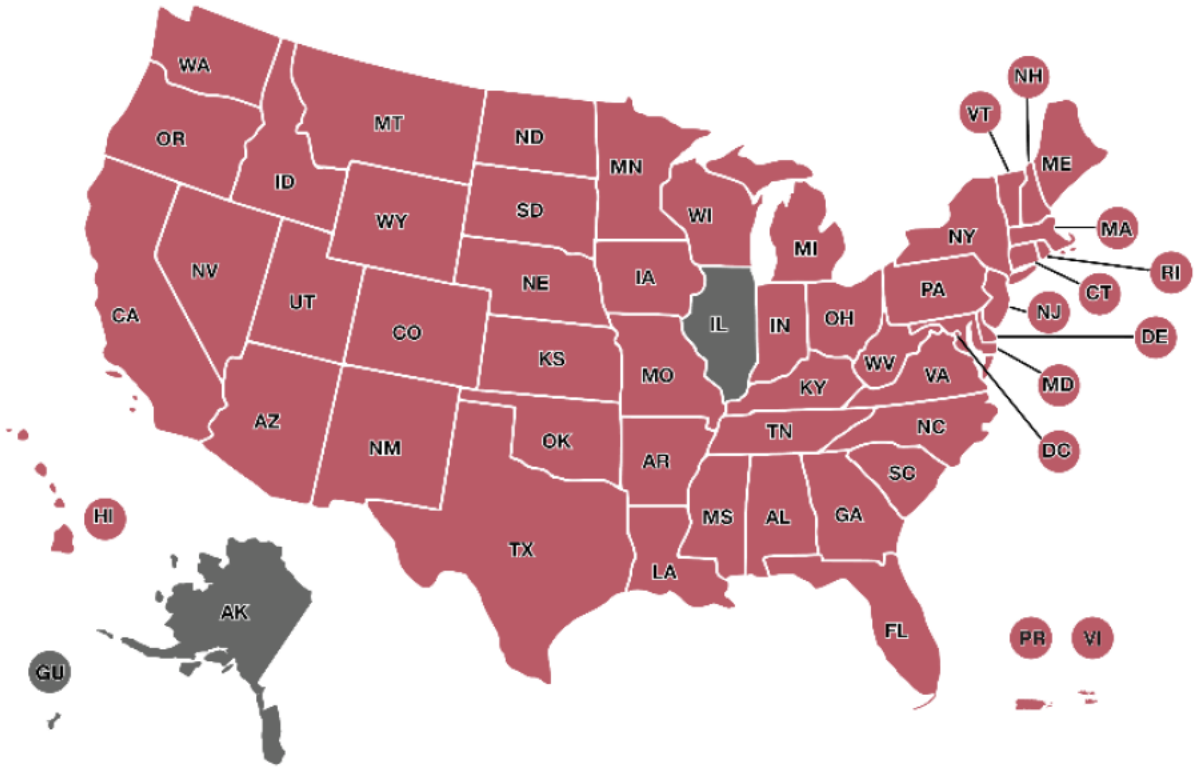
Message Keys: **NICB Impound/Export File Query (NIQ)**

Configured to Send this Query



Message Keys: **NICB All Files Query (NAQ)**

Configured to Send this Query



NHTSA
NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION



Section 47 Nlets WIKI

VIN Check



Web scrape service that provides Nlets users with information about a vehicle based on the decoding of the VIN.

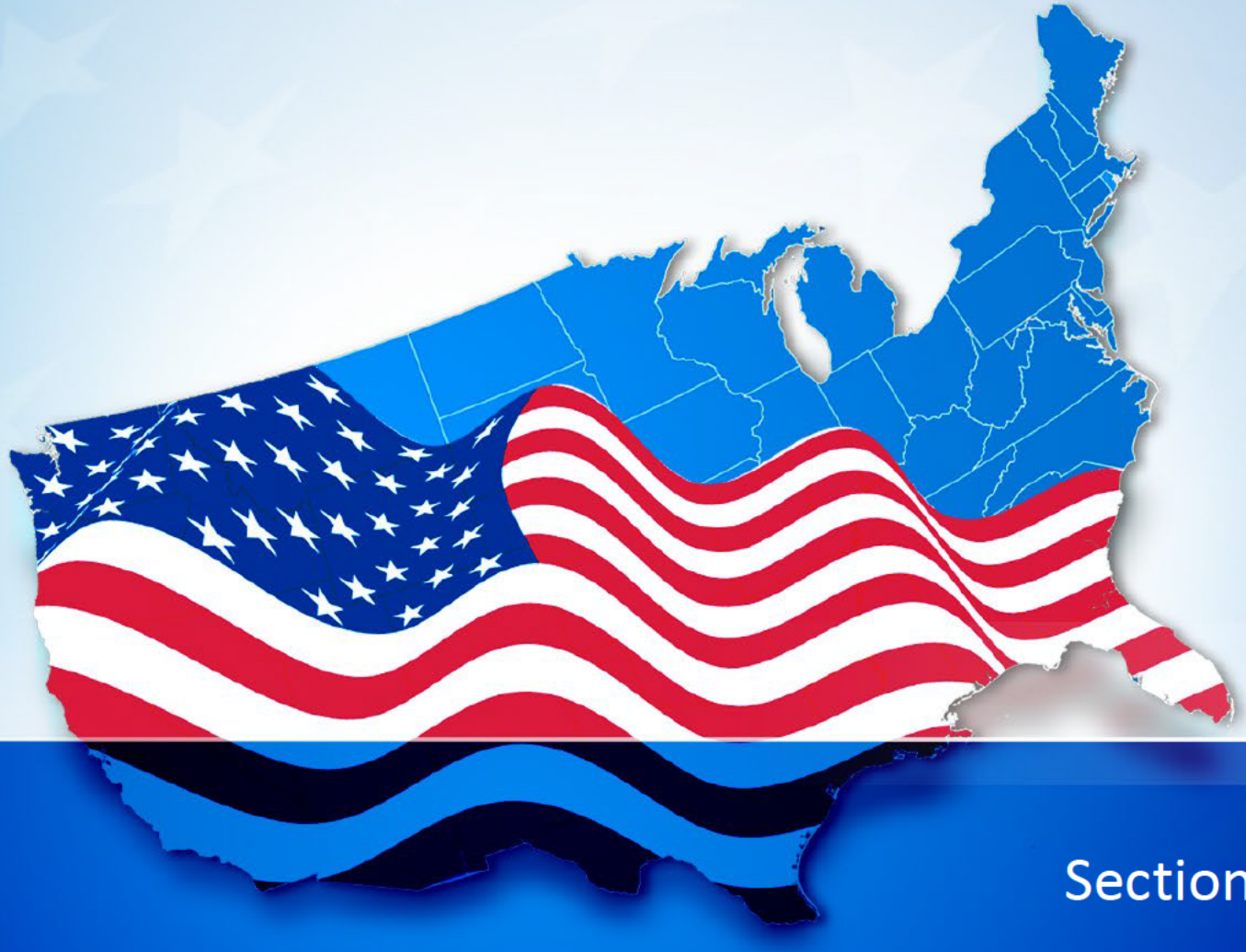




Users will receive specific vehicle details such as the vehicle ***type***, vehicle ***make***, vehicle ***model***, model ***year***, and ***much more***.

GVR.NL0000000.
13:00 09/28/2017 00038
13:00 09/28/2017 01106 616
AZNLETS46.TXT
VIN: 3GNEC12J48G183197
VEHICLE DATA
VIN: 3GNEC12J48G183197
Vehicle Type: MULTIPURPOSE PASSENGER VEHICLE (MPV)
Make: CHEVROLET
Make: GENERAL MOTORS LLC
Model: Avalanche
Model Year: 2008
Doors: 4
BodyClass: Pickup
EngineCylinders: 8
DisplacementCC: 5300.0
DisplacementCI: 323.42584370208
DisplacementL: 5.3
Doors: 4
DriveType: 4x2
EngineModel: LY5
GVWR: Class 2E: 6,001 - 7,000 lb (2,722 - 3,175 kg)
Make: CHEVROLET
Manufacturer: GENERAL MOTORS LLC
Model: Avalanche
ModelYear: 2008
PlantCity: Silao
Series: 1/2 Ton
Trim: LS
VehicleType: MULTIPURPOSE PASSENGER VEHICLE (MPV)
BrakeSystemType: Hydraulic
EngineConfiguration: V-Shaped
FuelInjectionType: Sequential Fuel Injection (SFI)
PlantCountry: Mexico
PlantCompanyName: GMNA
OtherEngineInfo: Active Fuel Mgt.
ErrorCode: 0 - VIN decoded clean. Check Digit (9th position) is correct
EngineManufacturer: GM
ManufacturerId: 984

OTHER DATA ABOUT THIS VIN RESPONSE:
Error Codes: 0 - VIN decoded clean. Check Digit (9th position) is correct

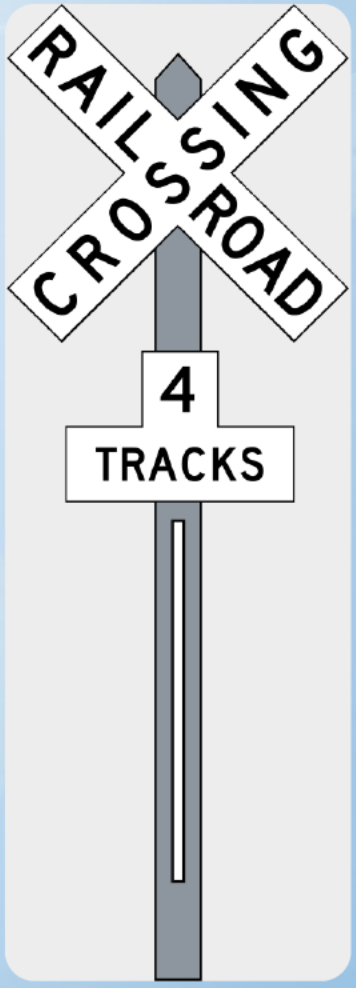


Section 45 Nlets WIKI

Railroad Crossing Transactions

Powered By Nlets

The purpose of this transaction is to make valuable railroad crossing information available to over one million Nlets users through their existing equipment and network connectivity.





Prior to this, law enforcement's access to the FRA database was through an Internet site:
http://safetydata.fra.dot.gov

When an accident or other event occurs at a railroad crossing, the Public Safety Answering Point (PSAP)/911 Center or the responding officer will need to have a ***working knowledge or the website AND have Internet access*** from their machine.



Nlets has obtained a copy of the FRA database and now allows access to it via the Nlets network.



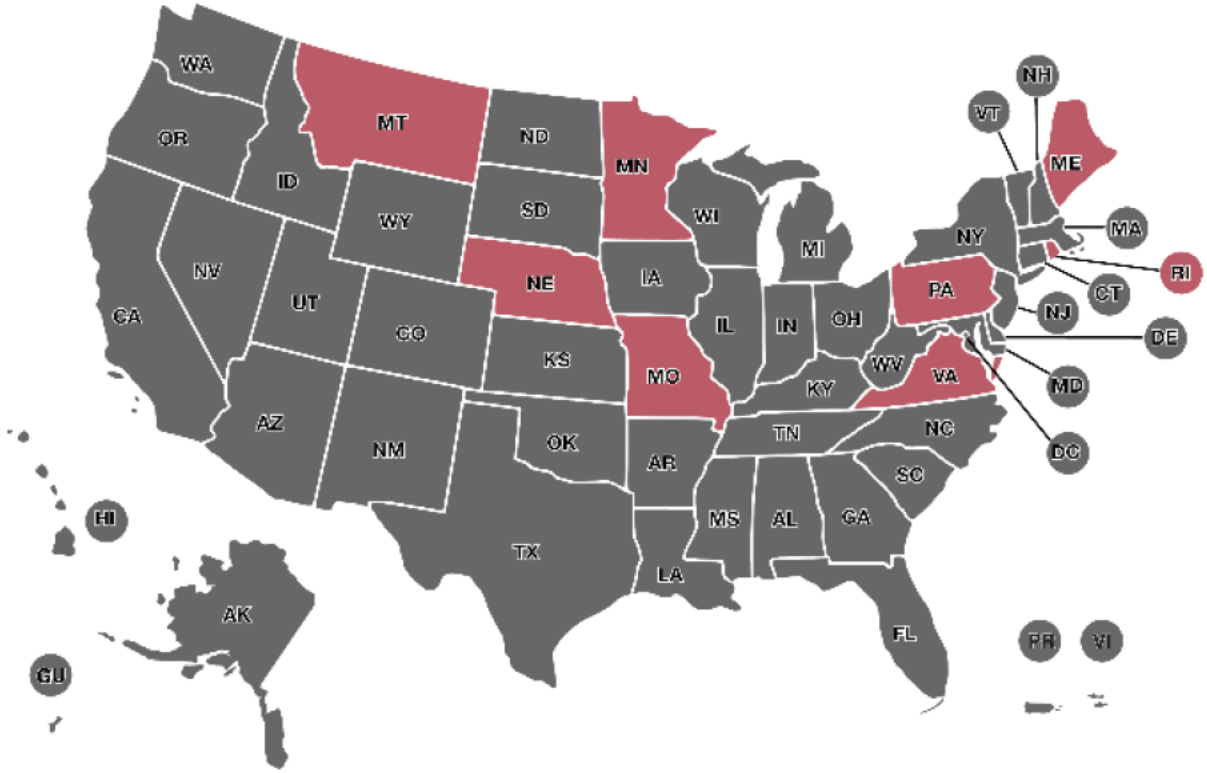
Because all railroad crossings have a number assigned to them, the ‘RCQ’ can be used to generate a response with all of the relevant crossing information:

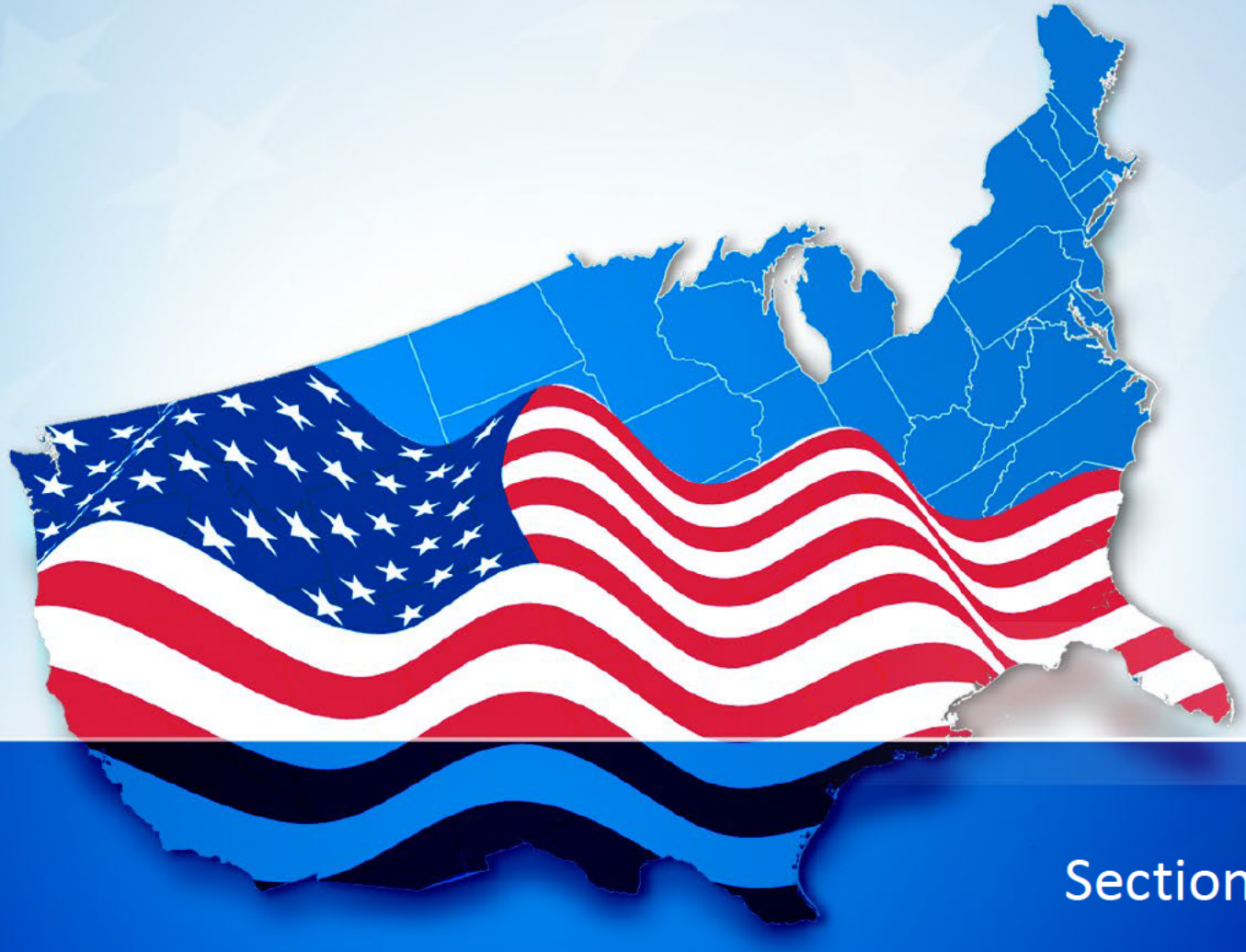
- Street information
- GPS coordinates for dispatch
- Railway contact information to stop services



Message Keys: **Railroad Crossing Query (RCQ)**

Configured to Send this Query





Section 41 Nlets WIKI

Alarm Exchange Transactions

Powered By Nlets

The purpose of the alarm exchange transaction is to help provide a standard message key for ***electronically transmitting information*** between an alarm monitoring company and a Public Safety Answering Point (PSAP).



Goal #1

Eliminate telephone calls between the alarm monitoring company and the 9-1-1 PSAP.



Goal #2

Eliminate miscommunication between the alarm monitoring company operators and the 9-1-1 PSAP call takers.



Goal #3

Decrease processing and response times to alarm-related calls-for-service with an increase in law enforcement apprehensions made, fires more quickly extinguished, and lives saved.







There are three primary uses for the ‘ALQ’ transaction:

- Initial notification of an alarm event
- Bi-directional update of ***status*** between an alarm monitoring company and the PSAP
- Bi-directional update of ***other events*** between an alarm monitoring company and a PSAP.

ASAP - Before

Takes up to 8 minutes with the possibility of errors!

Bu

before

ASAP - After

The business/home alarm alerts the alarm monitoring company.

The alarm company's system electronically gathers the required data then sends it to the ASAP where the 'ALQ' is generated and sent to Nlets.

Takes only SECONDS with no errors!



Approved CSA's

Secured by ADT

UCC EXCEPTIONAL

DIEBOLD

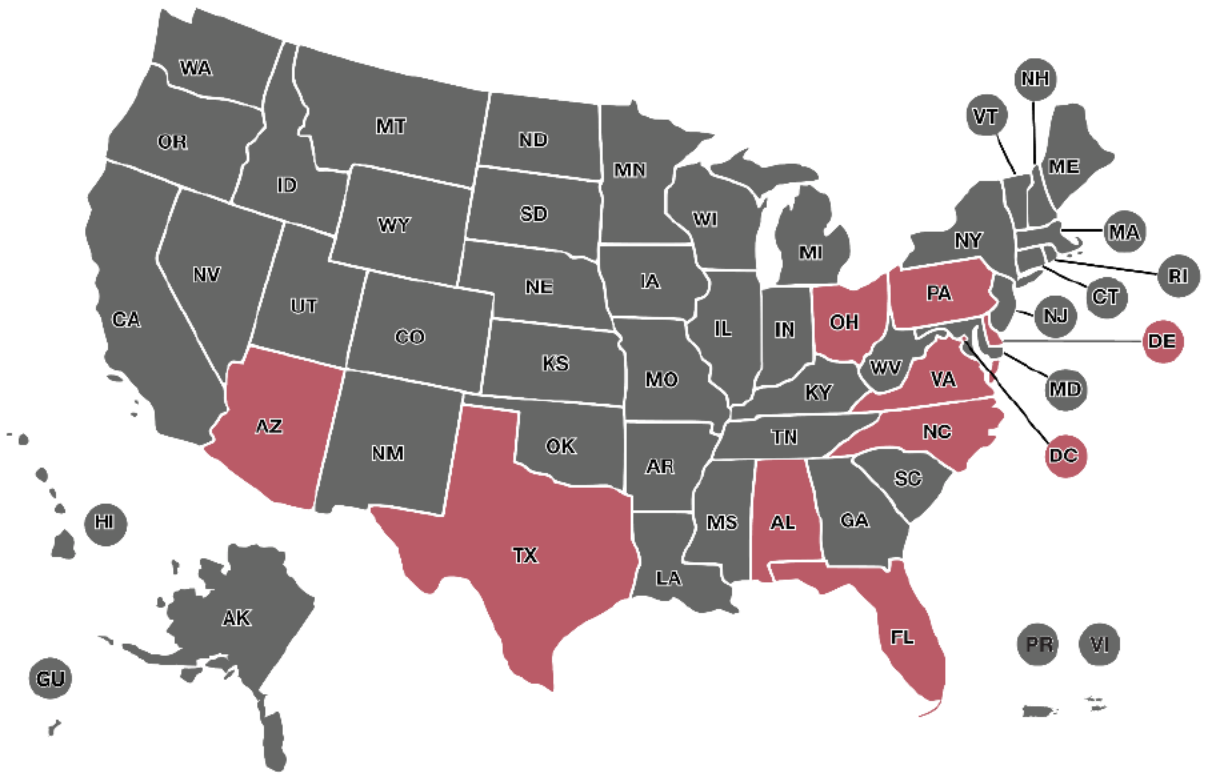
VECTOR SECURITY

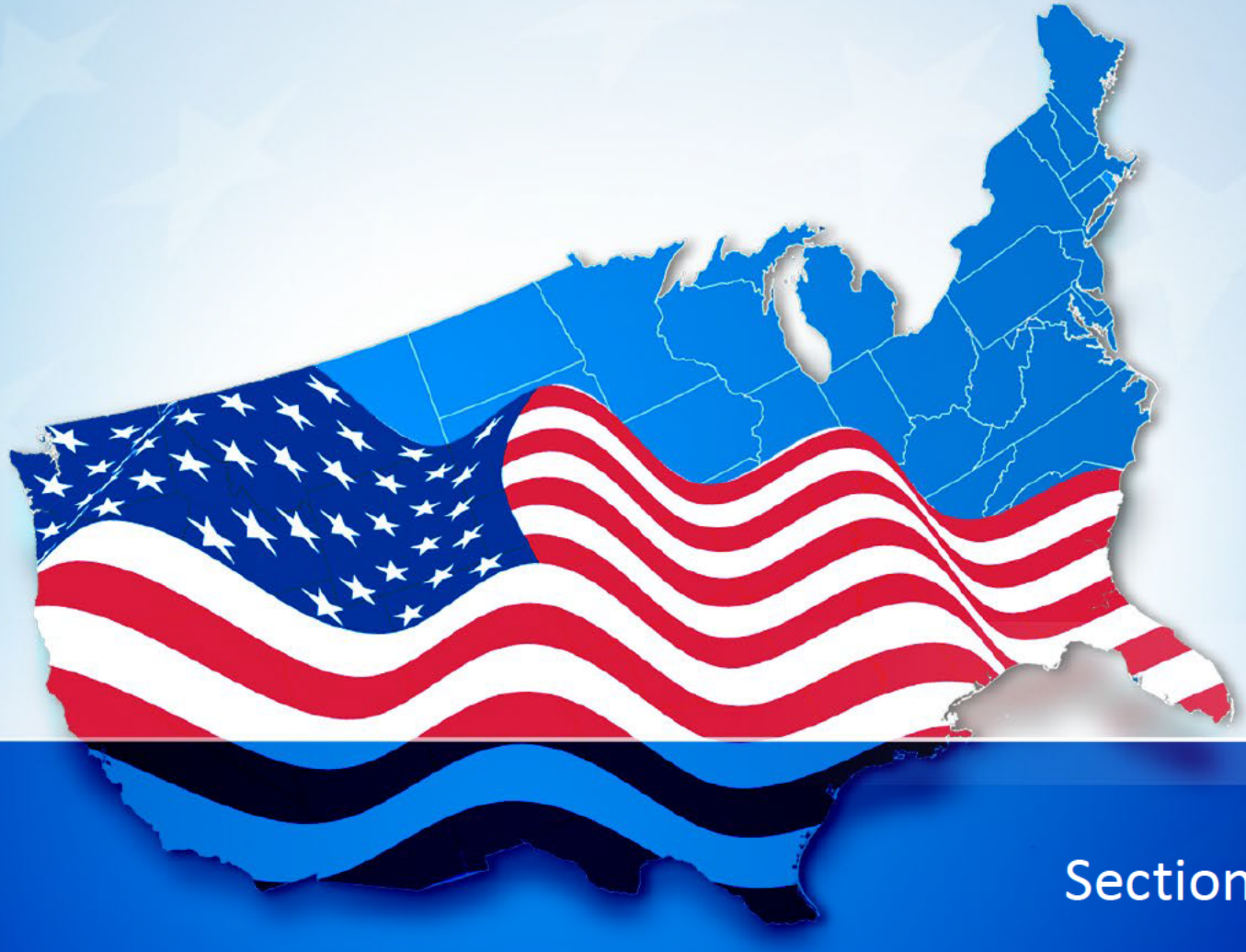
Monitronics™

Rapid Response
Safeguard
Affiliated
RFI
American Alarm
Protection One
Stanley
Guardian
CMS
ADS – Nashville
California Security – Safeguard
Central Security Group
Vivint
NMC

Message Keys: **Alarm Exchange Query (ALQ)**

Implemented





Section 30 Nlets WIKI

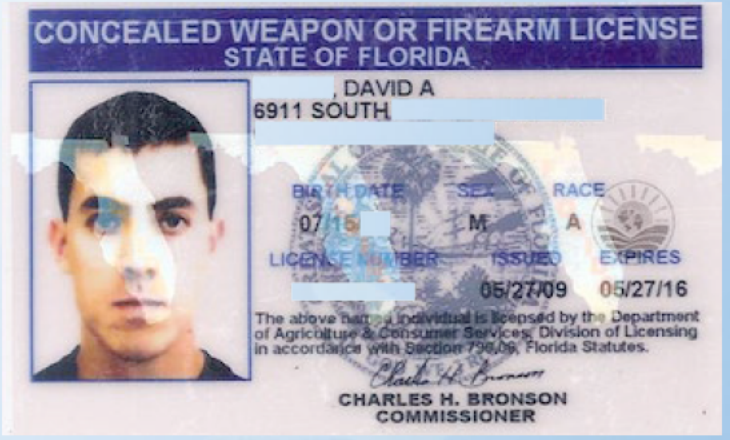
Concealed Weapons Permit Information

Powered By Nlets



The purpose of the concealed weapons permit information system is to provide ***a standardized, secure, and efficient method*** for states that have an automated concealed weapons permit system ***to respond automatically*** to requests from other states over Nlets.

A response will be returned with the notification that a permit ***does*** or ***does not exist***, its ***status***, and a ***description of the owner***.





Users must recognize that each state will deal with the searching of their database their own way.

For example, some states may not support a search using the SSN. Others may support the SSN but not by Name and DOB.



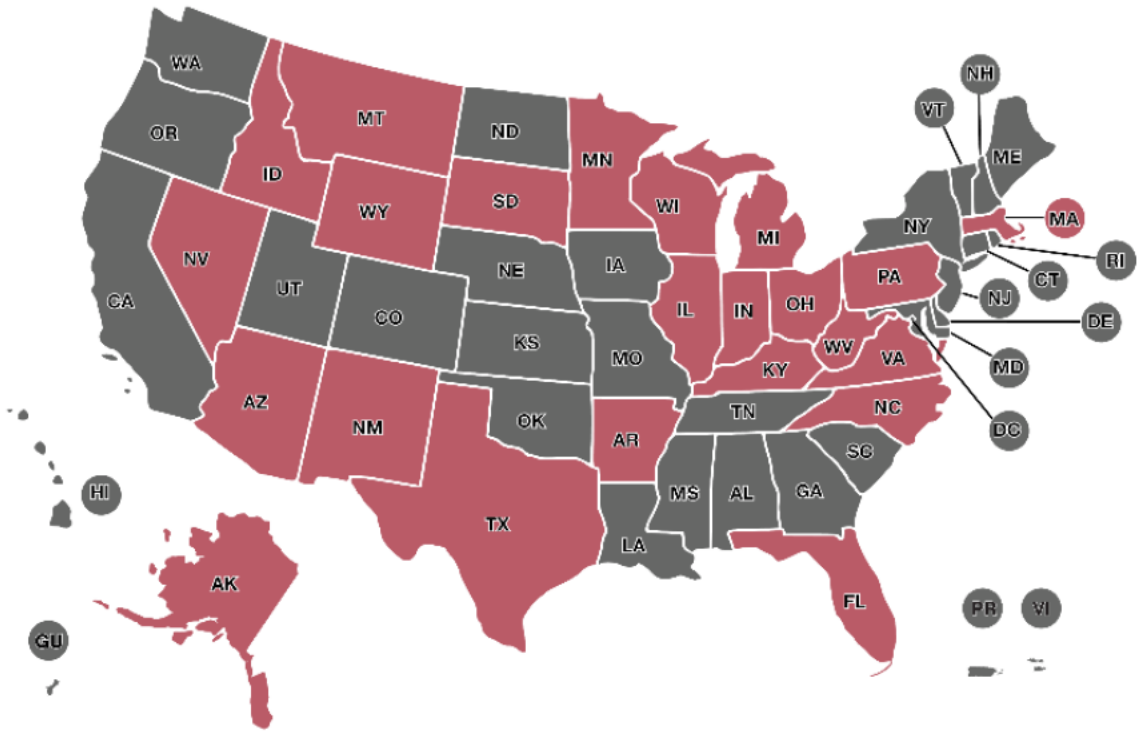
Details on the unique way states will search their concealed weapons database may be found in their HELP file.

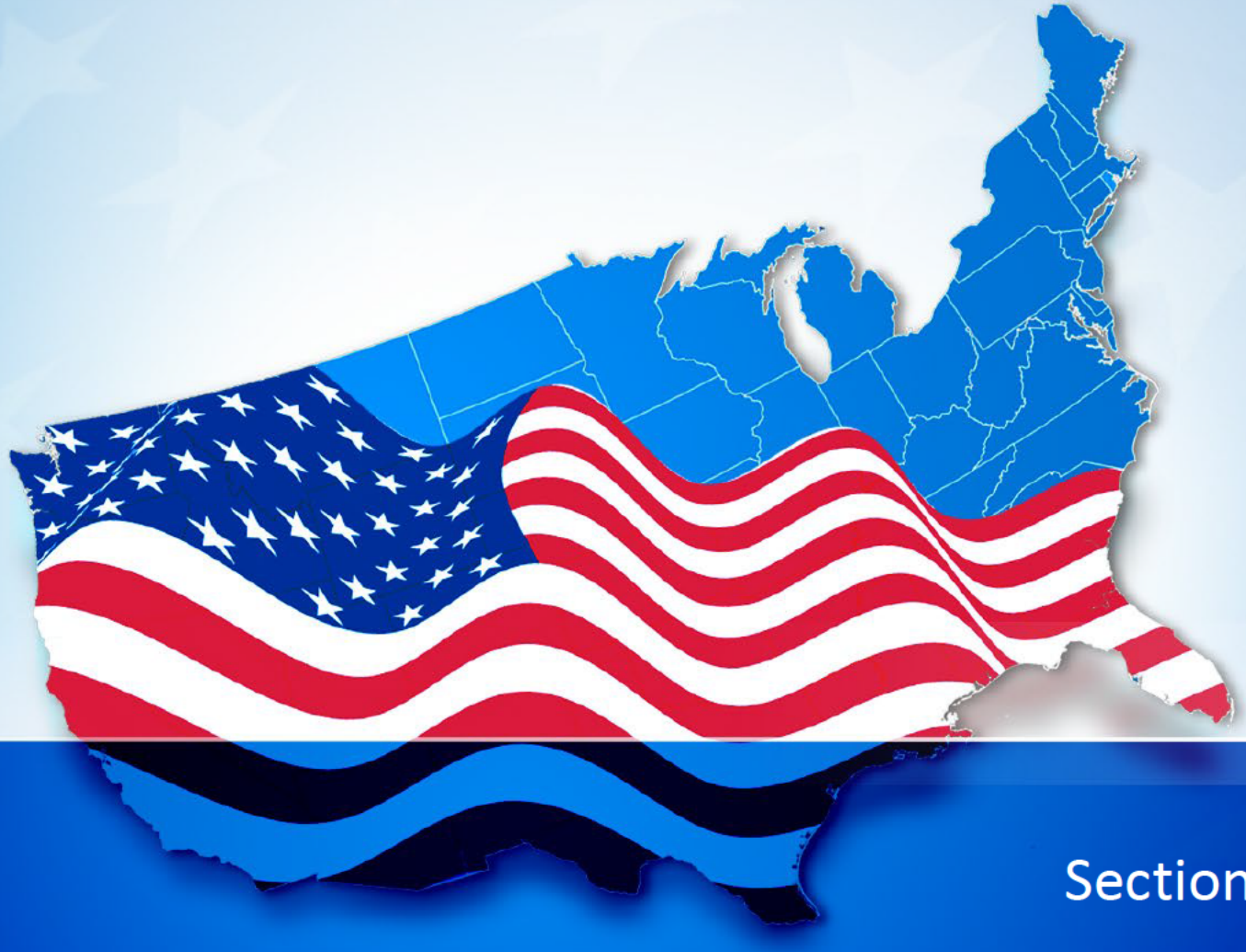
To obtain a record, send an AM to a 9-character ORI where the first two characters are the state code followed by "GUNHELP"

Example:
To access Minnesota's HELP record, the destination ORI would be "**MN**GUNHELP."

Message Keys: **Concealed Weapons Query (CWQ)**

Database accessible to Nlets users





Section 18 Nlets WIKI

Sex Offender Registration Transactions

Powered By Nlets

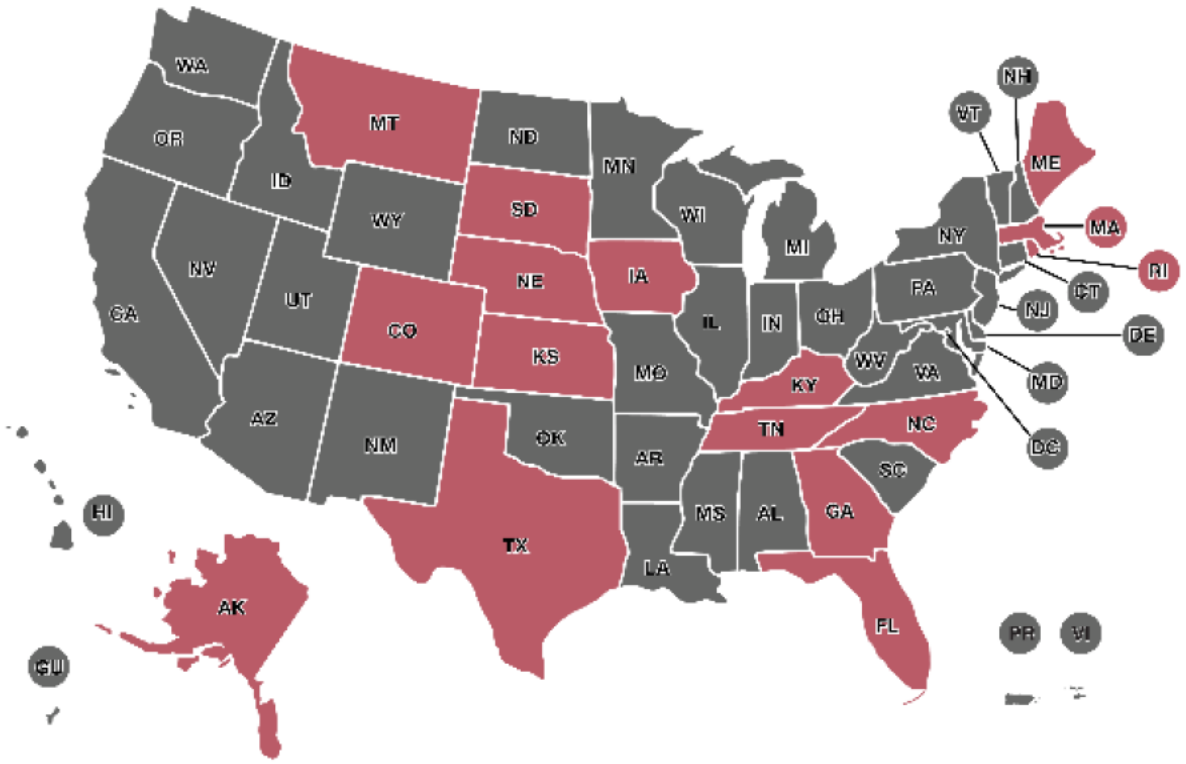
This transaction allows an agency to request out-of-state sex offender registration records.

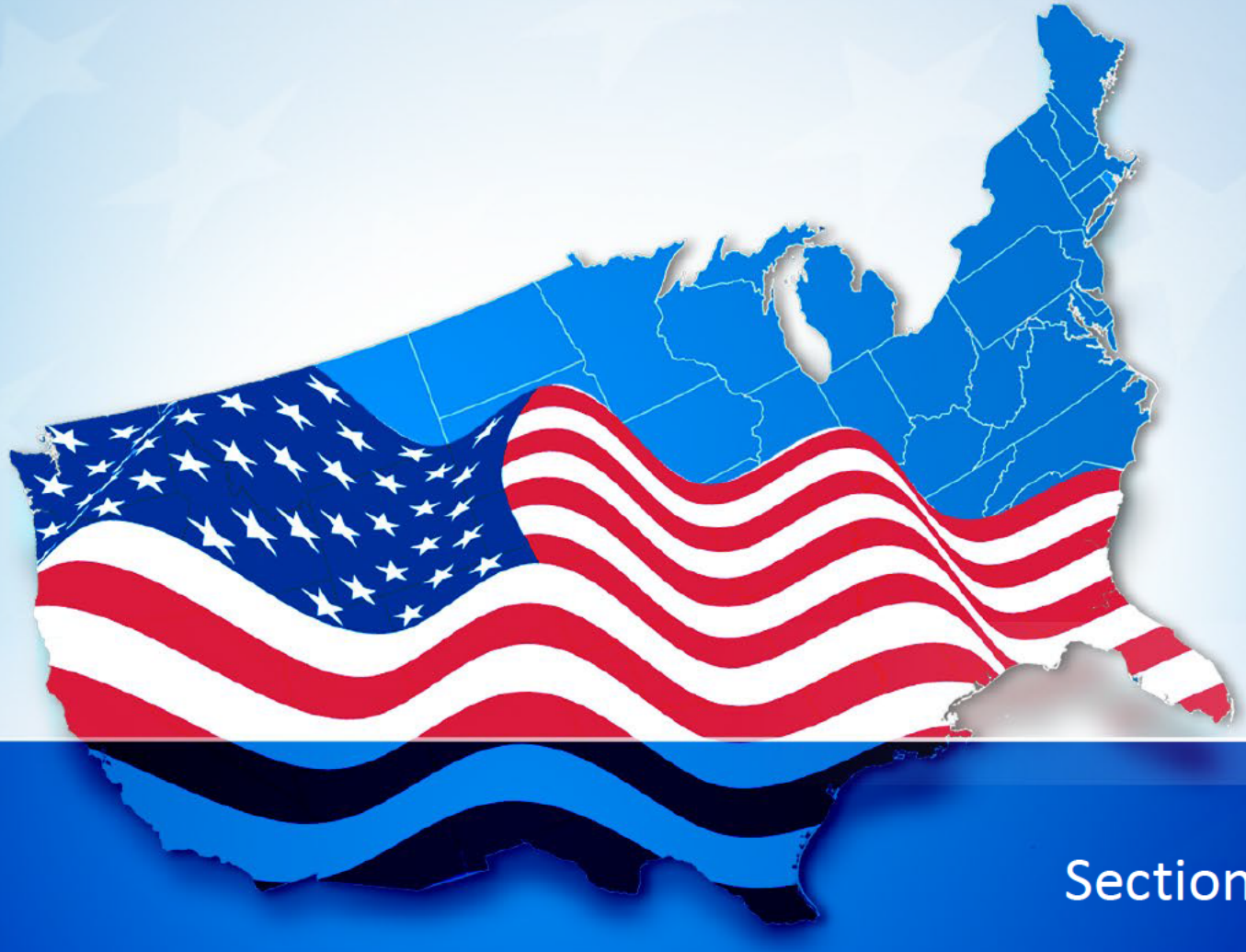
Only criminal justice agencies authorized to access criminal records will be allowed to submit an ‘SOQ’ to Nlets.



Message Keys: **Sex Offender Query (SOQ)**

Database accessible to Nlets users





Section 31 Nlets WIKI

Wildlife Violation and License File

Powered By Nlets

The purpose of this transaction is to provide a standardized, secure, and efficient method for Nlets users to ***exchange wildlife violator and license information***.





This would be done primarily between conservation officers and, secondarily, between state, local, and federal law enforcement and criminal justice agencies.



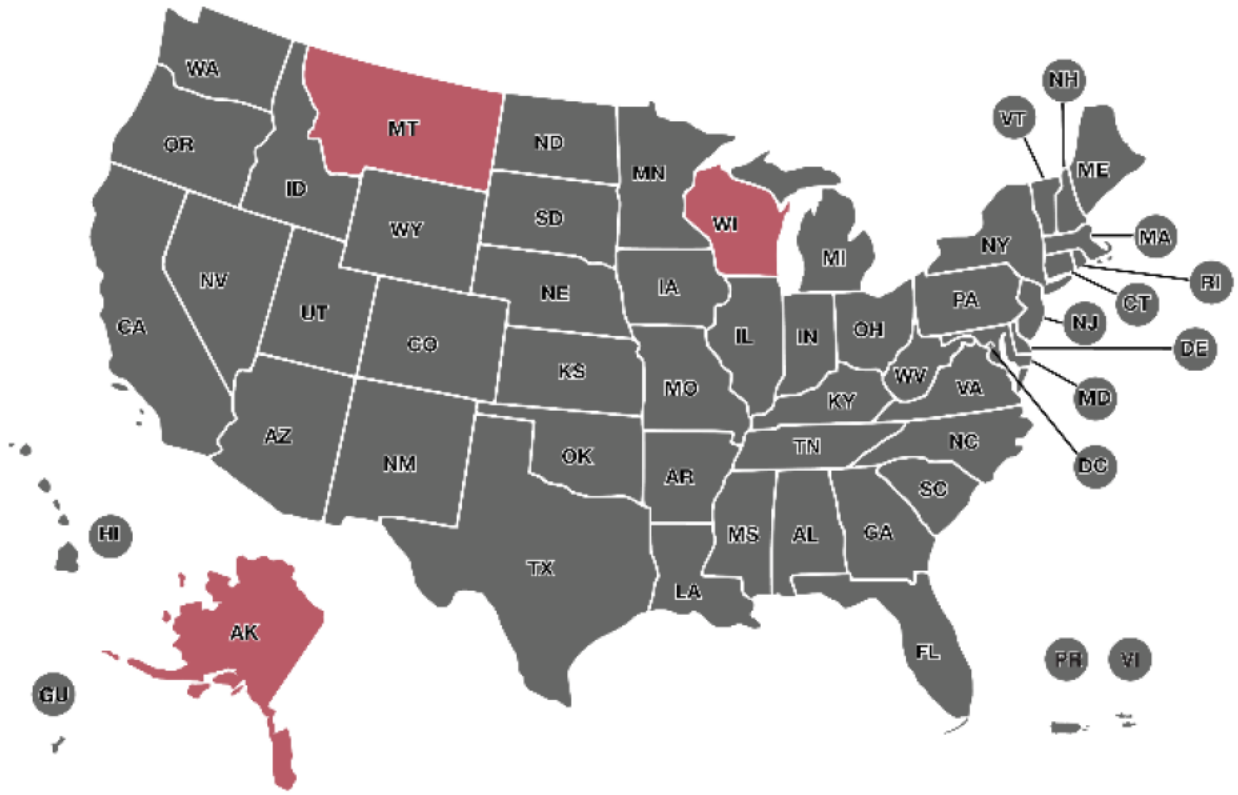
The response will be returned with the ***violator and/or license information***.

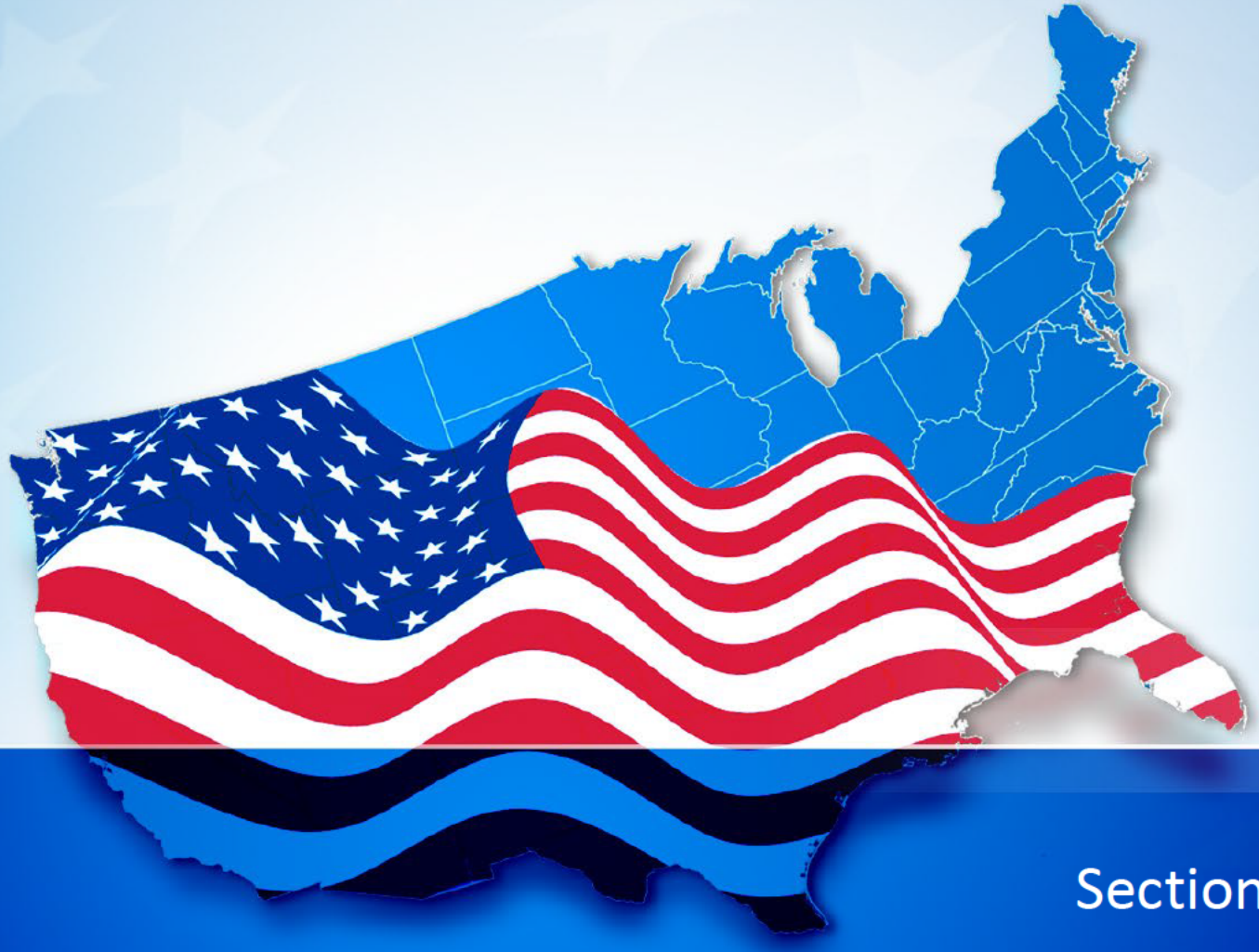
The requester will review the response and contact the agency of record if more details are needed.



Message Keys: **Wildlife Violation Query (WLQ)**

Database accessible to Nlets users





Section 32 Nlets WIKI

Communicating with Canada



Powered By Nlets





Nlets supports a computer-to-computer interface to Canada for the purposes of exchanging criminal justice related information.





The Canadian Police Information Centre (CPIC) is a system similar to the FBIs NCIC system.

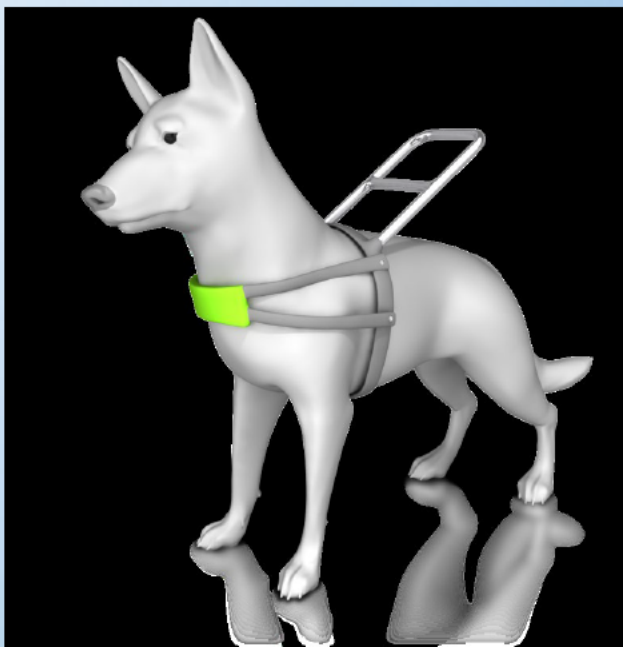


Canadian Article File (CAQ)

Once you confirm that the article is the correct article reported ***it can be impounded*** pending specific instructions from the Canadian agency that entered the article into the CPIC system.







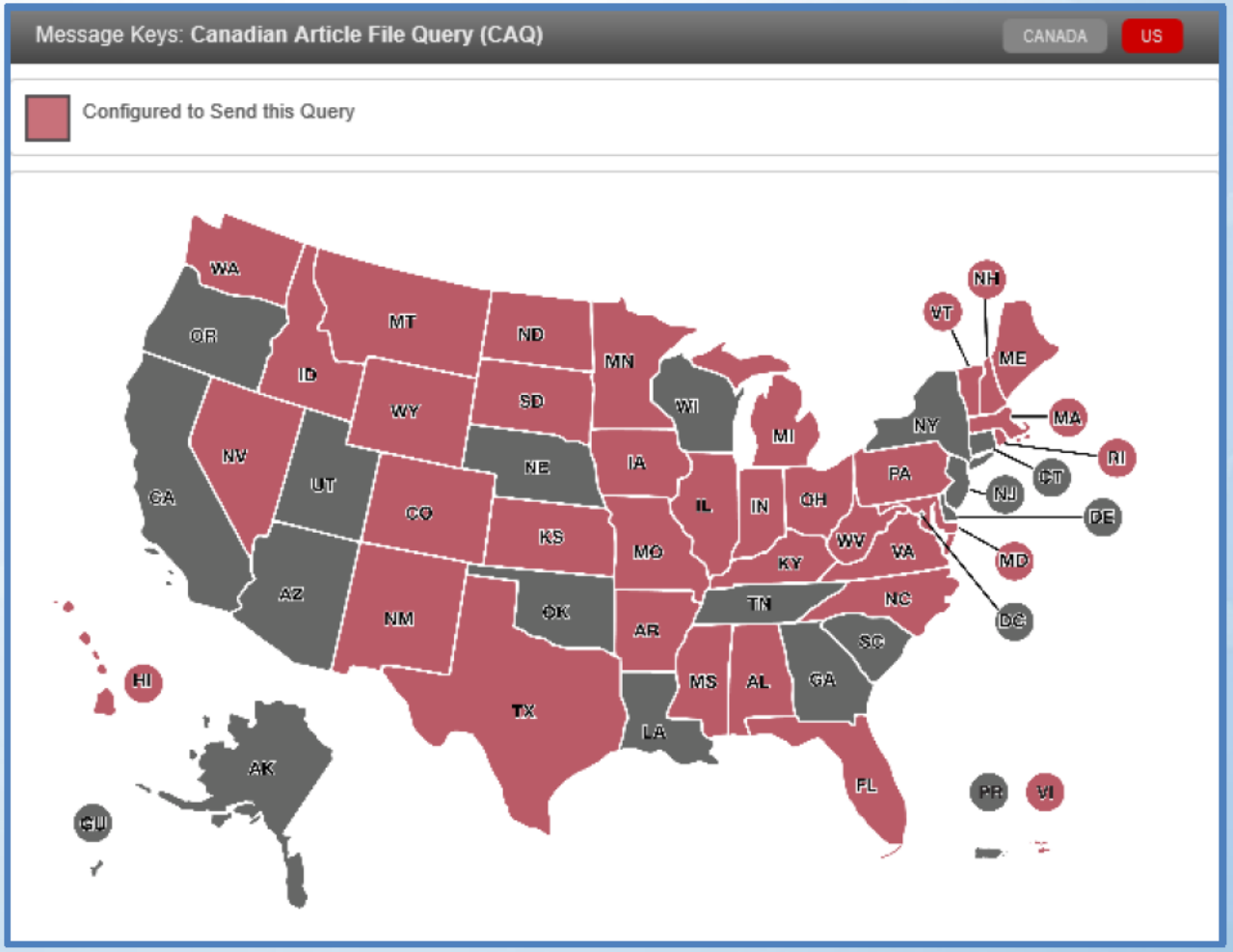
There may be occasions when the article record is associated with other records in the CPIC system. These will be returned as part of the initial response.





The types of records that are available to U.S. users from the CPIC Article File:

- Stolen
- Recovered/Found/Seized
- Lost/Missing
- Pawned/Loaned


Message Keys: Canadian Article File Query (CAQ)
CANADA
US
Configured to Send this Query
WA
OR
CA
ID
NV
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MS
MI
IN
KY
TN
AL
OH
WV
GA
FL
SC
NC
VA
PA
NY
MD
DE
NJ
CT
RI
MA
VT
NH
ME
DC
PR
VI
AK
HI
GU



Canadian Boat File (CBQ)



CPIC defines a boat as a watercraft, which may be a small open vessel, a large vessel, or ship propelled by oars, sails, or engines.



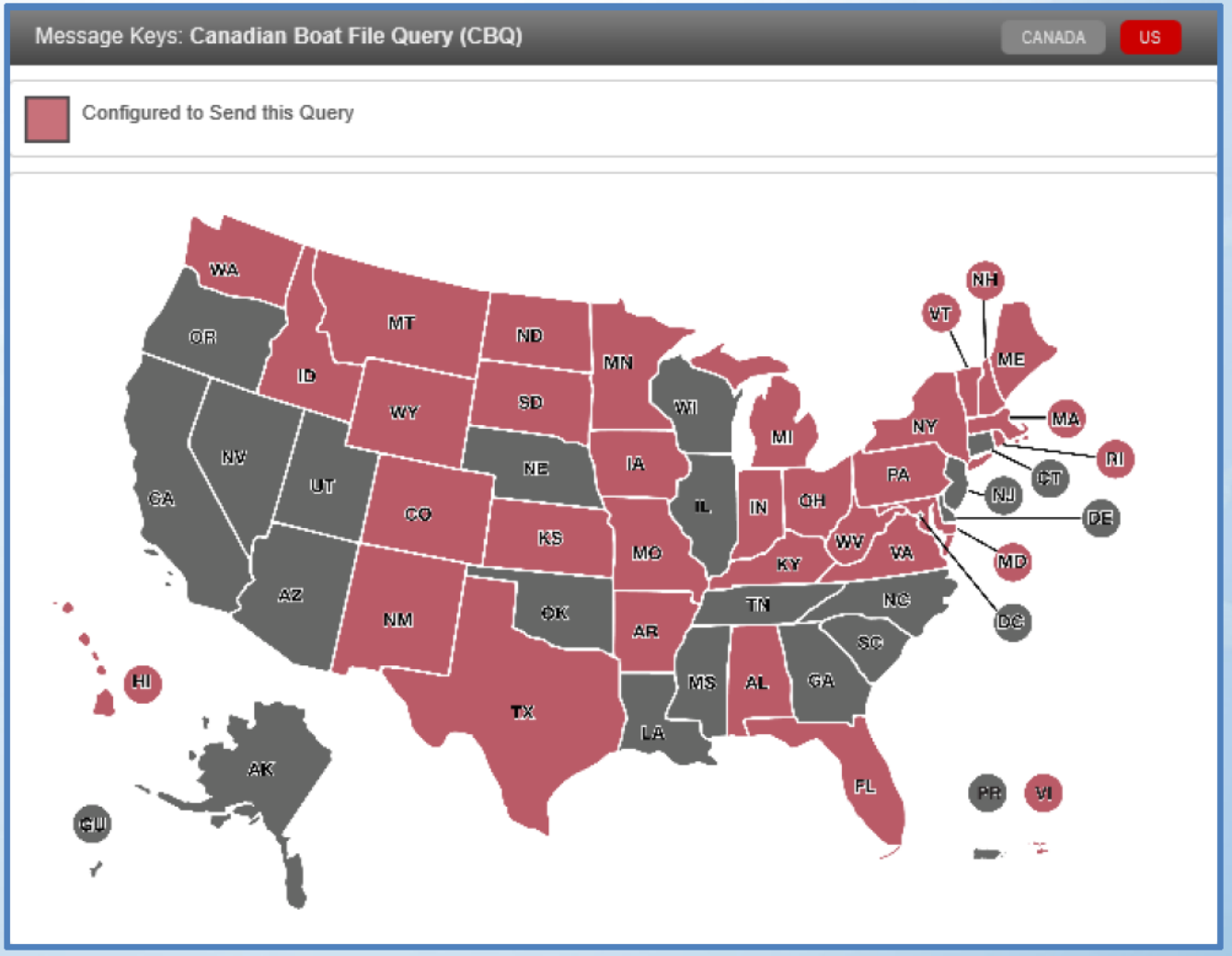
Users may also query the Canadian boat file for information on ***stolen boat motors*** by using the serial number.





The types of records that are available to U.S. users from the CPIC Boat File:

- Stolen
- Abandoned
- Missing


Message Keys: Canadian Boat File Query (CBQ)
CANADA
US
Configured to Send this Query
WA
OR
CA
ID
NV
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MS
MI
IN
KY
TN
AL
OH
WV
GA
FL
SC
NC
VA
PA
NY
MD
DE
NJ
CT
RI
MA
VT
NH
ME
DC
AK
HI
GU
PR
VI



Canadian Gun File (CGQ)



CPIC defines a gun as any barreled weapon that can discharge a bullet or other missile, or any imitation of such a weapon.







Examples of the types of guns allowed into this file:

- Revolvers or Pistols
- Rifles
- Shotguns
- Flints/Caps/Matchlock Muz
- Automatic Weapons/Machi
- Signal Flares/Rockets/Gas G
- Air Guns



Each inquiry to the Canadian gun file will check the ***stolen gun file*** and the Canadian ***gun registration file***.









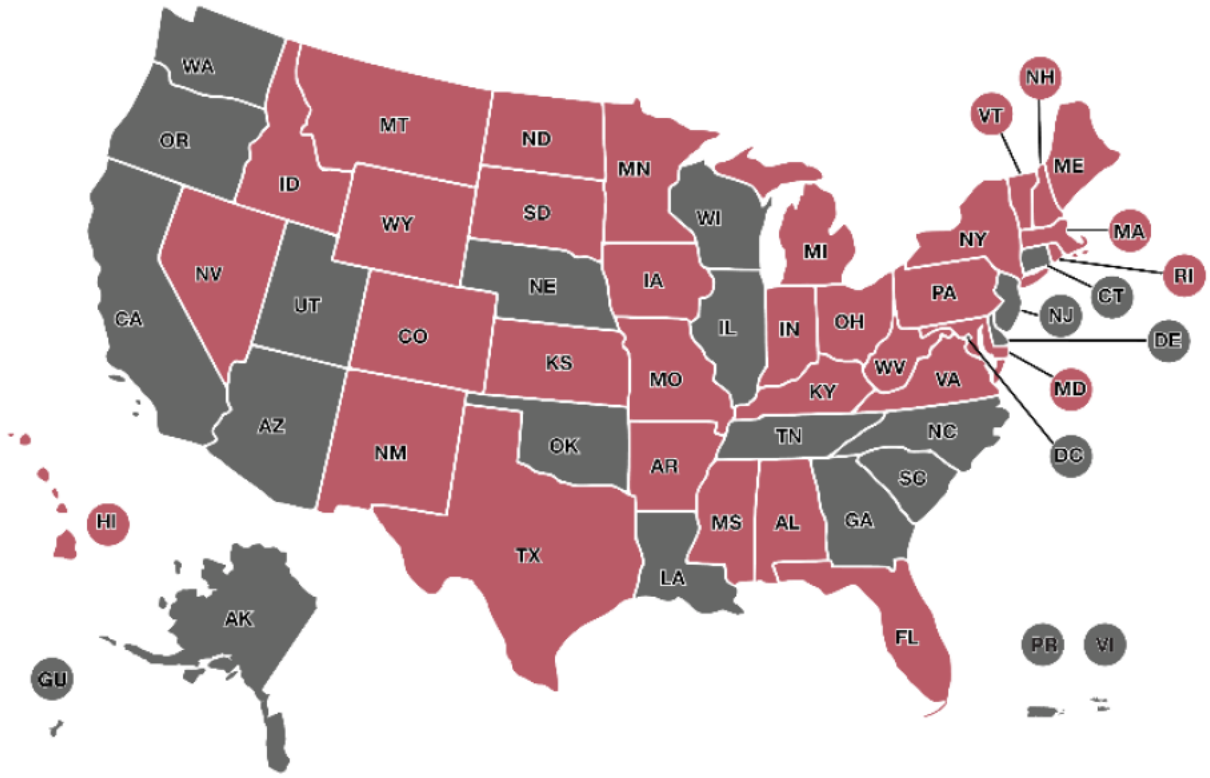
The types of records that are available to U.S. users from the CPIC Gun File:

- Stolen
- Recovered
- Lost/Missing
- Pawned/Loaned

Message Keys: **Canadian Gun File Query (CGQ)**

CANADA | US

Configured to Send this Query





Canadian Securities File (CSQ)

Examples of the types of securities allowed into this file:

- BD – Corporate bonds and debentures issued by corporations
- CC – Canadian issued currency
- CU – Foreign issued currency
- ID – Stolen, lost, or fraudulent identification documents
- MO – Money orders or traveler's checks
- PP – Canadian and foreign passports
- SB – Federal, provincial, and municipal bonds and debentures
- ST – Stocks
- VD – Vehicle documents
- OT – All other security documents





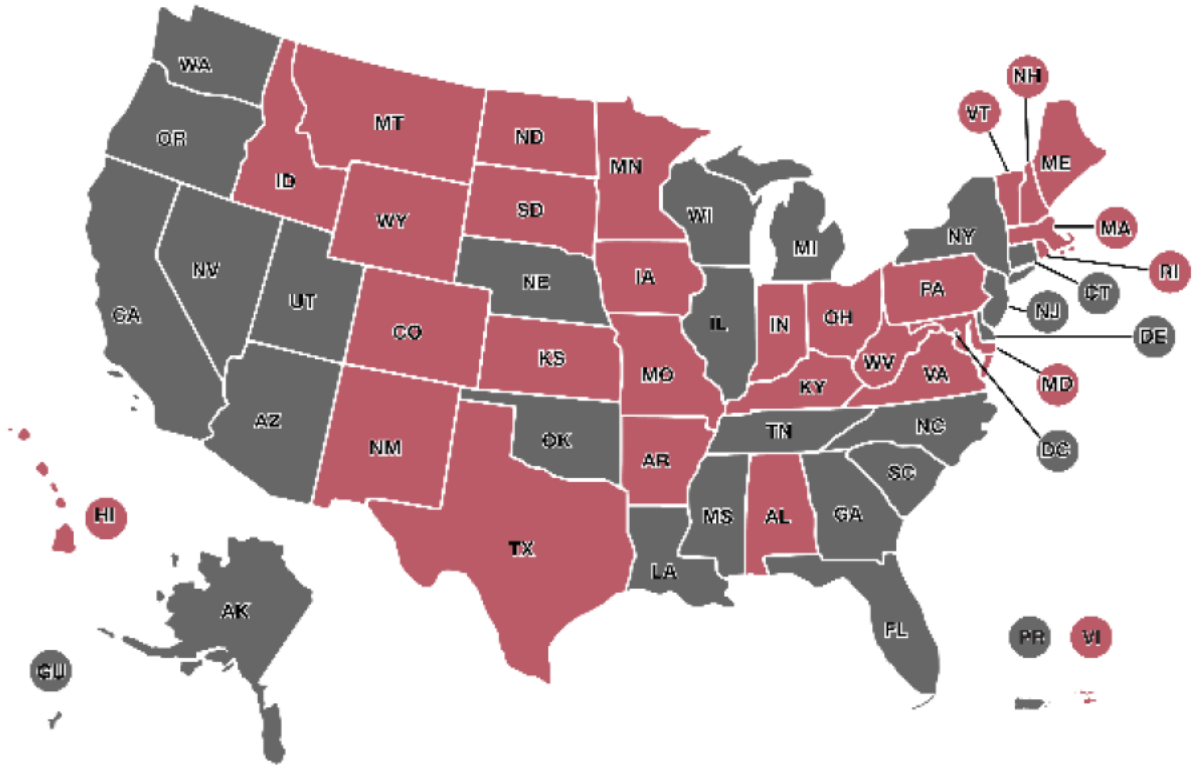


The types of records that are available to U.S. users from the CPIC Securities File:

- Stolen
- Counterfeit
- Lost/Missing
- Pawned/Loaned
- Fraudulent/Recovered

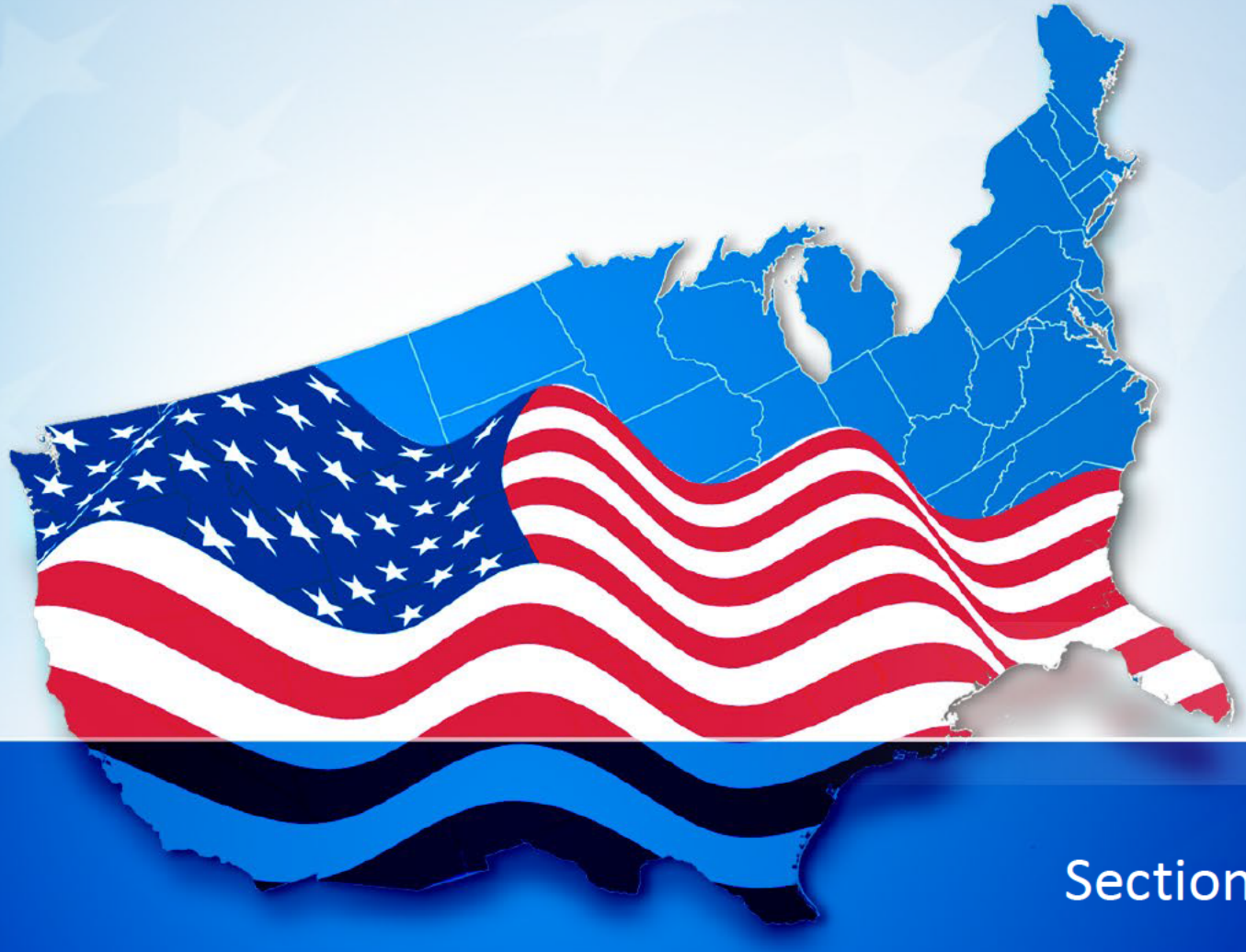
Message Keys: **Canadian Securities File Query (CSQ)**

Configured to Send this Query



Additional Canadian Files

UQ - Canadian Driver License
WQ - Canadian Person's File – Wanted
VQ - Canadian Vehicle File
XQ - Canadian Vehicle Registration File



Section 38 Nlets WIKI

LEO Flying Armed

Powered By Nlets

To obtain a copy of the LEO Flying Armed HELP file, send and AM to destination "NLFLYHELP"



Sample Message to TSA

```
AM.PASO12345.VAFAM0199.*0008000001.TXT
LEOFA
NAM/SMITH, JOE.
AGY/ARIZONA POLICE DEPARTMENT.
BCN/BSO123456.
OFC/STATE.
NAO/WASHINGTON, GEORGE.
CRT/YES.
CPN/7031234989.
APN/2023456789.
EIT/PRISONER.
EIN/SMITH, JOHN.
NOA/AMERICAN AIRLINES.
FLN/AA1234.
DOF/122508.
DAP/TSA.
CAP/TSA.
FDA/TSA.
```

Explanation of Fields:

BCN – Badge or Credential Number
OFC – Officer Type (State or Local)
NAO – Name of Authorizing Official
CRT – Completed Training (yes/no)
CPN – Cell Phone Number
APN – Agency Phone Number
EIT – Escorted Individual Type
EIN – Escorted Individual Name
NOA – Name of Airline
FLN – Flight Number
DOF – Date of Flight
DAP – Departure Airport
CAP – Connecting Airport
FDA – Final Destination Airport

Fields With Notable Changes

*NAO – Name of Authorizing Official

- The authorizing official will be the Chief, Sheriff, or Agency Administrator of the law enforcement department that endorses and approves the submission of the LEO Flying Armed Nlets message.

*EIT – Escorted Individual Type

- Now called the EXPLANATION OF INDIVIDUALS TRAVEL
- Explanations must be exactly ***one word*** with no added spaces or punctuation (*ProtectiveDetail, *Surveillance, *Enforcement, *Investigation, *Prisoner)

*EIN – Escorted Individuals Name

- If the LEO will not be escorting an individual the field must be formatted EIN/. (or) EIN/NA

Fields With Notable Changes

*FLN – Flight Number

- Multiple flight numbers should be separated by a comma and a space
- Include all flight numbers if there are layovers

*CAP – Connecting Airport

- Must be a known federalized U.S. three-character airport code
- This field is not required if no connections are scheduled
- Use CAP/TSA for all test queries

Sample TSA Response

AM.VAFAM0199
07:41 01/03/2011 05854
07:41 01/03/2011 01488 AZNLETS20
TXT
FLYING ARMED LEO REQUEST APPROVED.
YOUR UNIQUE LEOLANE IDENTIFIER IS: AAA11111
NAME: SMITH, JOE
AGENCY: ARIZONA POLICE DEPARTMENT
BADGE/CREDENTIAL: BS0123456
NAME OF AUTHORIZING OFFICIAL: WASHINGTON, GEORGE
COMPLETED TRAINING: YES
CELL PHONE: 7031234989
ESCORTED INDIVIDUAL: SMITH, JOE
DEPARTING AIRPORT: TSA
CONNECTING AIRPORT: TSA
FINAL DESTINATION AIRPORT: TSA
AIRLINE: AMERICAN AIRLINES
FLIGHT NUMBER: AA1234
FLIGHT DATE: 122508
PRINT OUT THIS REPLY AND PRESENT IT AT THE AIRPORT'S LEO LANE



Activity

- Pair Up
- Discuss what data sources you'd like to see made available via Nlets
  - Suggested data source currently exists?
    - Who owns the data?
- Share with the group



Nlets Initiatives & Projects



DHS 5 Eyes Project

Powered By Nlets





What exactly is 5 Eyes?

An intelligence alliance of five countries bound by the multilateral UKUSA Agreement, which is a treaty for joint cooperation in signals intelligence.





The DHS 5 Eyes Project will open up access to the DHS IDENT database for law enforcement via the Nlets network leveraging a new message key.

Projecting fall 2017



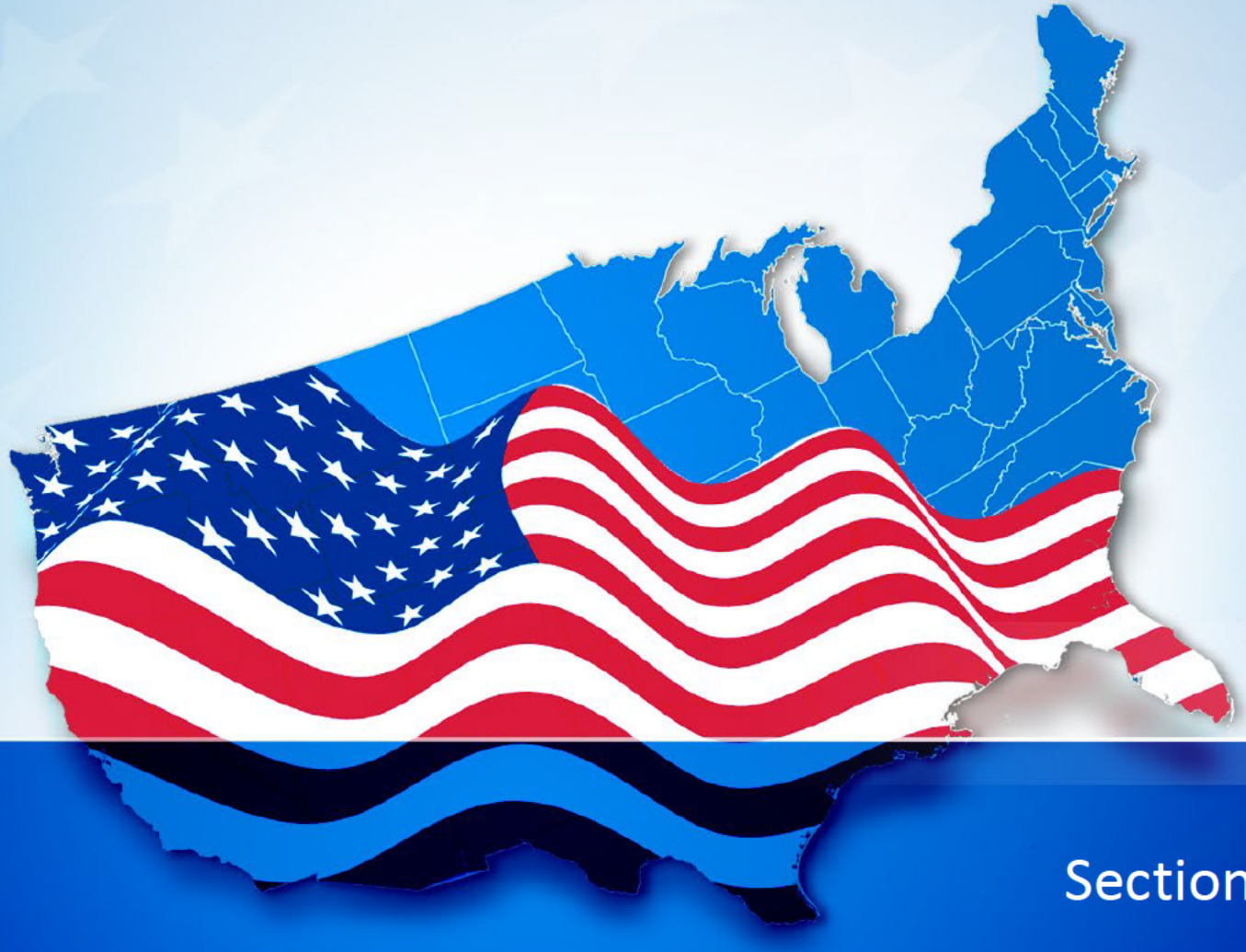
Parsing Service

Powered By Nlets

Parsing

Nlets Parsing Services Include:

- Criminal History
- Stolen Vehicle Feed
- Registration Responses
- Multi-state Queries with no-hit suppression
  - State Warrants (complete)
  - Sex Offender Registration (by September 2017)
  - Wildlife Licensing (by September 2017)
  - CHRI Identity (by September 2017)
- Driver License



Section 37 Nlets WIKI

State Warrant Transactions

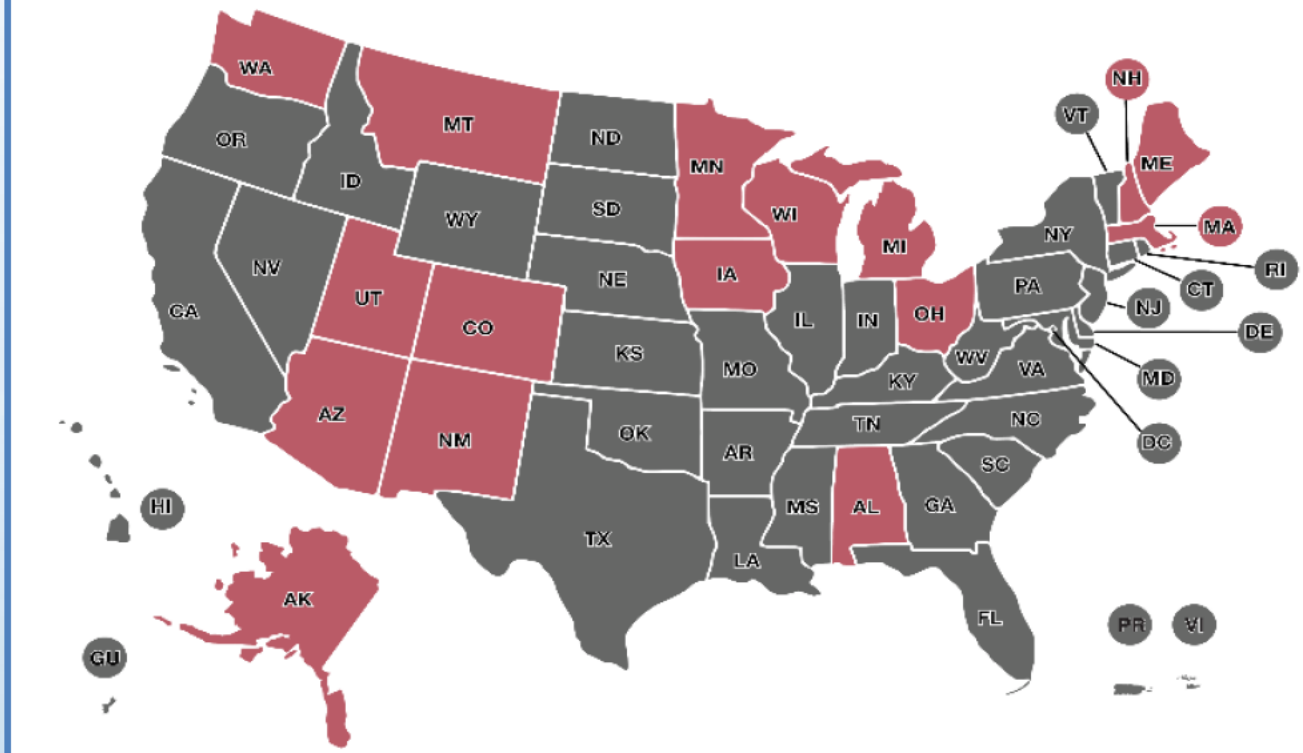
Powered By Nlets





Message Keys: **State Warrant Query (SWQ)**

Database accessible to Nlets users



Parsing

Nlets Parsing Services Include:

- Criminal History
- Stolen Vehicle Feed
- Registration Responses
- Multi-state Queries with no-hit suppression
  - State Warrants (complete)
  - Sex Offender Registration (by September 2017)
  - Wildlife Licensing (by September 2017)
  - CHRI Identity (by September 2017)
- Driver License

Developed in partnership with the U.S. Department of State, Passport Services, Nlets now provides the option for users to receive fully tagged, NIEM formatted driver license responses from all states via our message parsing service.



Responses (DRs) destined to an ***individual terminal*** or an ***entire state*** can be redirected to the message parsing service to be converted to a parsed driver license response (PDR).







Non-standard/unfamiliar formats require more careful review to interpret data

FOLLOWING IS THE NEVADA DMV RESPONSE FOR YOUR QUERY ON: OLN: 1030273456
*** DRIVER INFORMATION ***
NAME: DOE, TRACY JEAN RECORD STATUS: CURRENT SOC: 730784828 DOB: 04281980 SEX: F HGT: 504 WGT: 115 HAI: BRO EYE: BRO MAILING ADDRESS: 123 MAIN ST CITY/STATE/ZIP: HENDERSON, NV 890157519
PHYSICAL ADDRESS: CITY/STATE/ZIP: ,

*** DRIVER LICENSE INFORMATION ***
OLN: 1030273456 DUPLICATE: D RECORD STATUS: CURRENT LAST TRANSACTION: 07071998 MEDICAL CERTIFICATE STATUS CODE: NOT APPLICABLE NON-COMMERCIAL LICENSE CLASS: C TYPE: INSTRUCTION STATUS: SURRENDER EXPIRES: 04051998 RESTRICTIONS: Other
ID CARD NUMBER : 1030273456 TYPE: NEVADA ID CARD STATUS: EXPIRED RECORD STATUS: CURRENT ISSUED: 04122009 EXPIRES: 04282012

*** DETAILED WITHDRAWL INFORMATION ***
WITHDRAWL LIC STATE: NV REASON: BLK INV WDRL TY RSN STATUS: Cleared BEGIN: 05261999 END: 05261999 REINSTATE: CLEARED: 05261999 TYPE: INVALID WDRL TYPE OF FT+ EXTENT: ALL LICENSE RETURNED: N COMMENTS: CONVERSION HEND MUNI 165176B NS CLD 051898 WITHDRAWL LIC STATE: NV REASON: BLK INV WDRL TY RSN STATUS: Cleared BEGIN: 05261999 END: 05261999 REINSTATE: CLEARED: 05261999 TYPE: INVALID WDRL TYPE OF FT+ EXTENT: ALL LICENSE RETURNED: N COMMENTS: CONVERSION HEND MUNI 165176A NI NS CLD 051898 ORIGINAL DOCUMENT ON FILE AT NEVADA DEPARTMENT OF MOTOR VEHICLES PER NRS 52.205(3)

NAME: TRACY JEAN DOE
PRIMARY CONTACT ADDRESS: 123 MAIN ST; SILVER CITY, NM 88061
DATE OF BIRTH: 1980-04-28
SSN: 730784828
HEIGHT: 504
WEIGHT: 115
EYE COLOR: HAZ
GENDER: FEMALE

DRIVER LICENSE DETAILS
DRIVER AUTHORIZATION ID: 1030273456
JURISDICTION AUTHORITY CODE: NM
ISSUE DATE: 2010-04-01
EXPIRATION DATE: 2020-04-01
DRIVER ENDORSEMENT: None
DRIVER LICENSE PERMIT QUANTITY: 0
DRIVER LICENSE NON-COMMERCIAL CLASS: D
DRIVER LICENSE NON-COMMERCIAL CLASS CODE: D
DRIVER LICENSE NON-COMMERCIAL STATUS: Invalid
DRIVER ORGAN DONOR: False



Your state switch must be XML ready and be able to receive the PDR message.

A stylesheet needs to be in place.

Parsing

NLets Parsing Services Include:

- Criminal History
- Stolen Vehicle Feed
- Registration Responses
- Multi-state Queries with no-hit suppression
  - State Warrants (complete)
  - Sex Offender Registration (by September 2017)
  - Wildlife Licensing (by September 2017)
  - CHRI Identity (by September 2017)
- Driver License



Criminal History Information Exchange Format

CHIEF

Office of Justice Programs
BJS Bureau of Justice Statistics

Powered By Nlets

XML = eXtensible Markup Language

NIEM = National Information Exchange Model

The first goal with this grant was to standardize the criminal history response that the state consumer receives using XML vocabulary based on NIEM.



The second goal was recidivism statistics. The project involved a requirement to turn the standardized criminal history information into researchable information.





It will make professionals more efficient by avoiding mistakes because of misinterpretations of out-of-state codes.

More accurate and timely identification of persons prohibited from:

- Firearm purchase
- Working with children
- Working with the elderly
- Working with the disabled





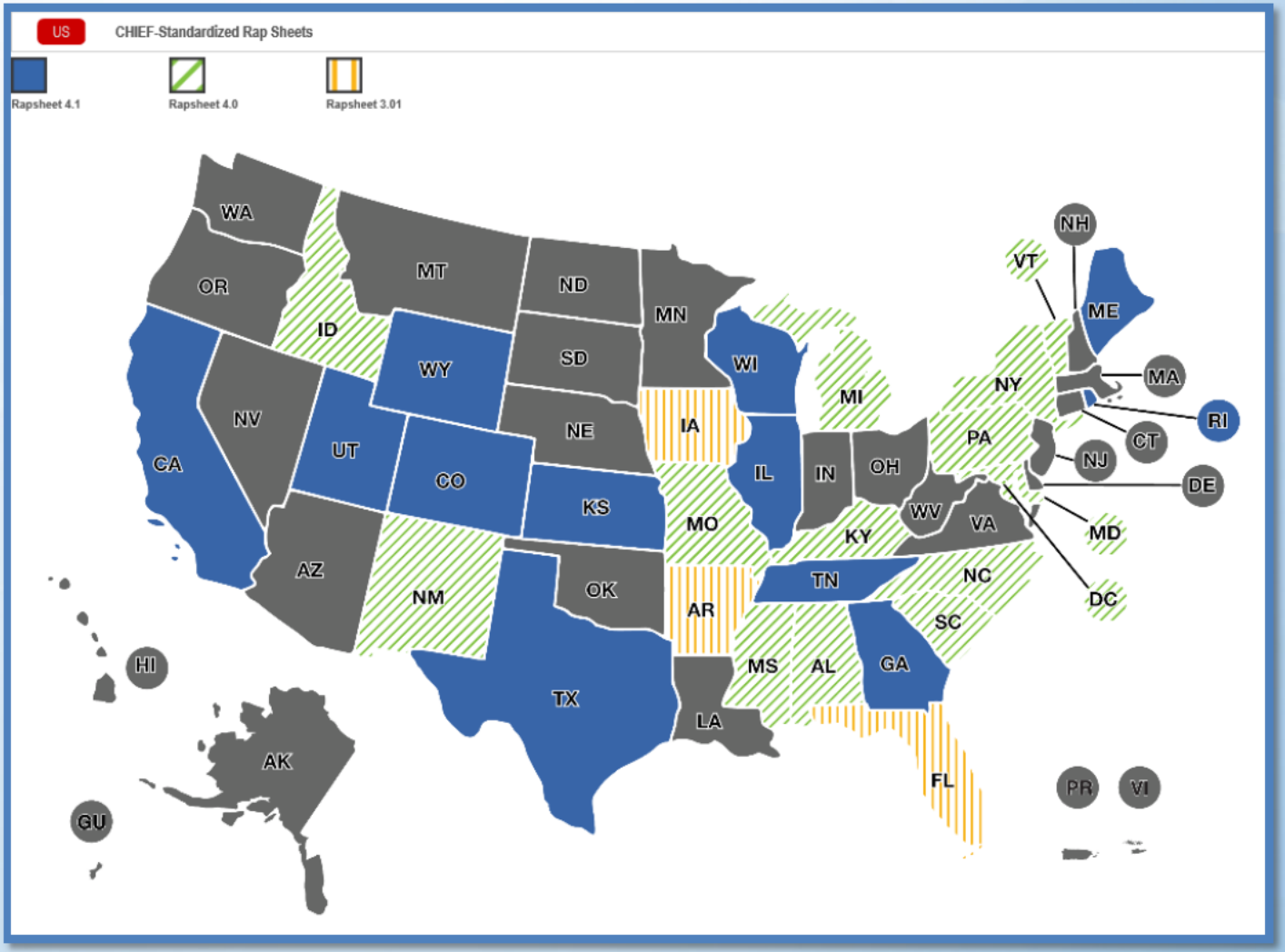
Better data for making decisions on:

- Detention
- Pre-trial Release
- Charge Enhancements
- Sentencing
- Correctional Classification



Streamlined background checks:

- National Security
- Employment
- Licensing


US
CHIEF-Standardized Rap Sheets
Rapsheet 4.1
Rapsheet 4.0
Rapsheet 3.01
WA
OR
CA
ID
NV
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MS
MI
IN
KY
TN
AL
OH
WV
GA
FL
SC
NC
VA
PA
NY
NH
VT
ME
MA
RI
CT
NJ
DE
MD
DC
PR
VI
HI
AK
GU



Nlets Interstate Sharing of Photos

NISP

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice
Research • Development • Evaluation

Homeland Security
Science and Technology

Powered By Nlets

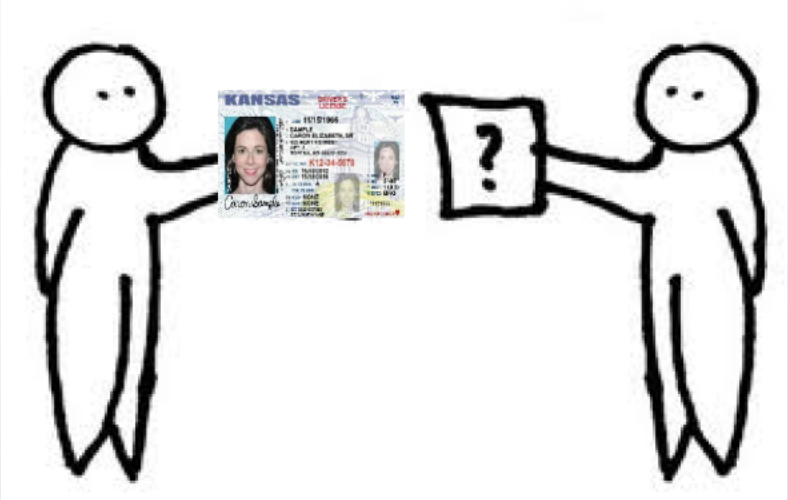
Nlets received support from the U.S. Department of Justice and the U.S. Department of Homeland Security ***to demonstrate the viability of exchanging interstate driver license photos*** among law enforcement and safety officials using Nlets.

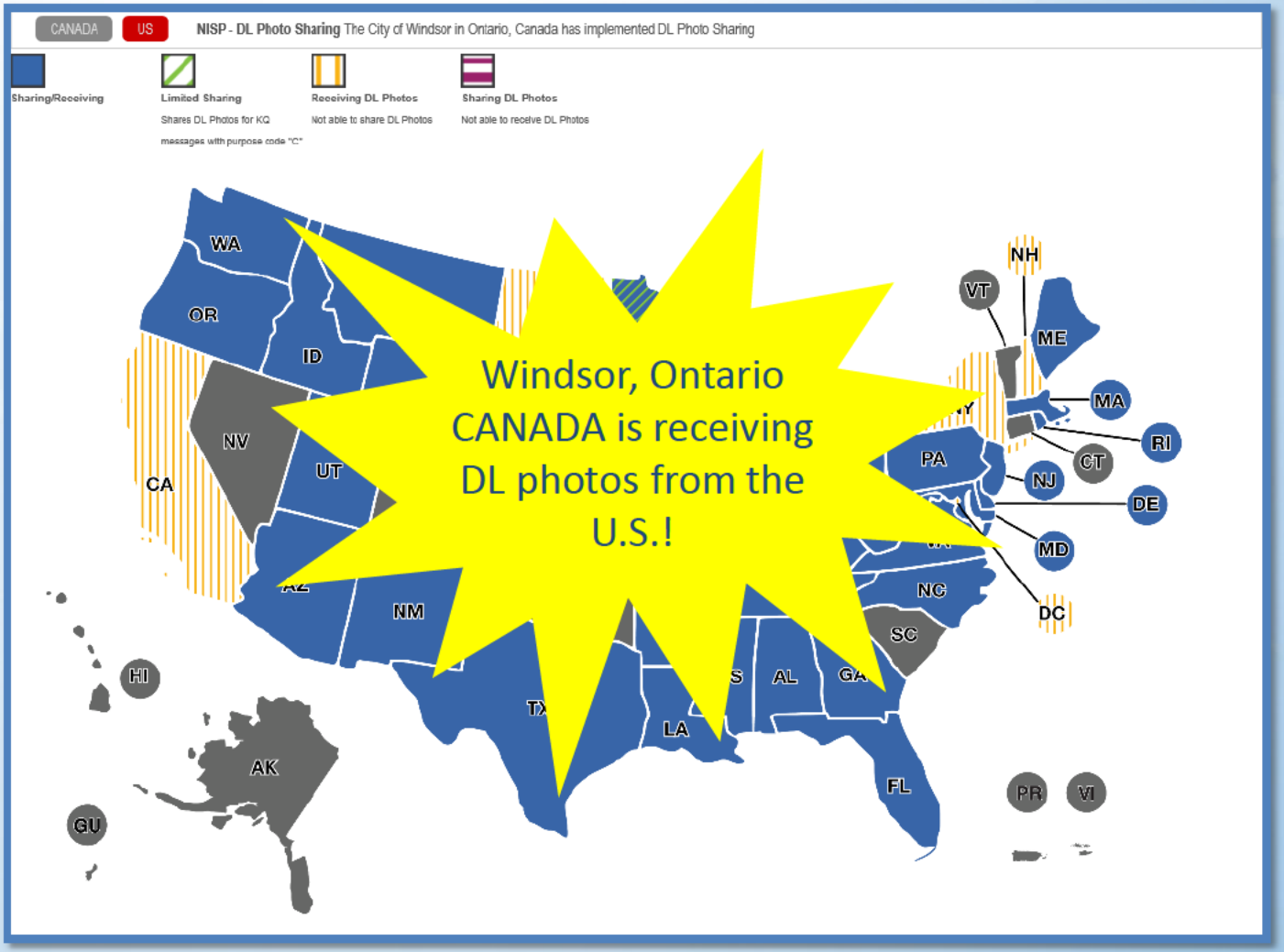


Over the past several years Nlets has implemented some form of driver license photo sharing in ***41 states!***



Sharing driver license photos nationwide will provide law enforcement with an additional tool they can use to verify a person is who they claim to be.




CANADA
US
NISP - DL Photo Sharing The City of Windsor in Ontario, Canada has implemented DL Photo Sharing
Sharing/Receiving
Limited Sharing
Shares DL Photos for KQ messages with purpose code "C"
Receiving DL Photos
Not able to share DL Photos
Sharing DL Photos
Not able to receive DL Photos
Windsor, Ontario CANADA is receiving DL photos from the U.S.!
WA
OR
ID
NV
CA
UT
NM
HI
AK
GU
TX
LA
AL
GA
FL
SC
NC
PA
NH
VT
ME
MA
RI
CT
NJ
DE
MD
DC
PR
VI



Nationwide Corrections Images and Information over Nlets

NCIEN

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice
Research • Development • Evaluation

Homeland Security
Science and Technology

Powered By Nlets



The purpose of the NCIEN project is to make corrections photos available to law enforcement and public safety officers over the Nlets network.



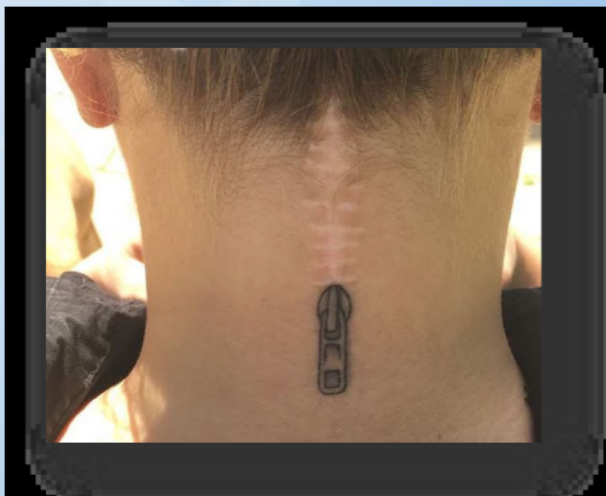


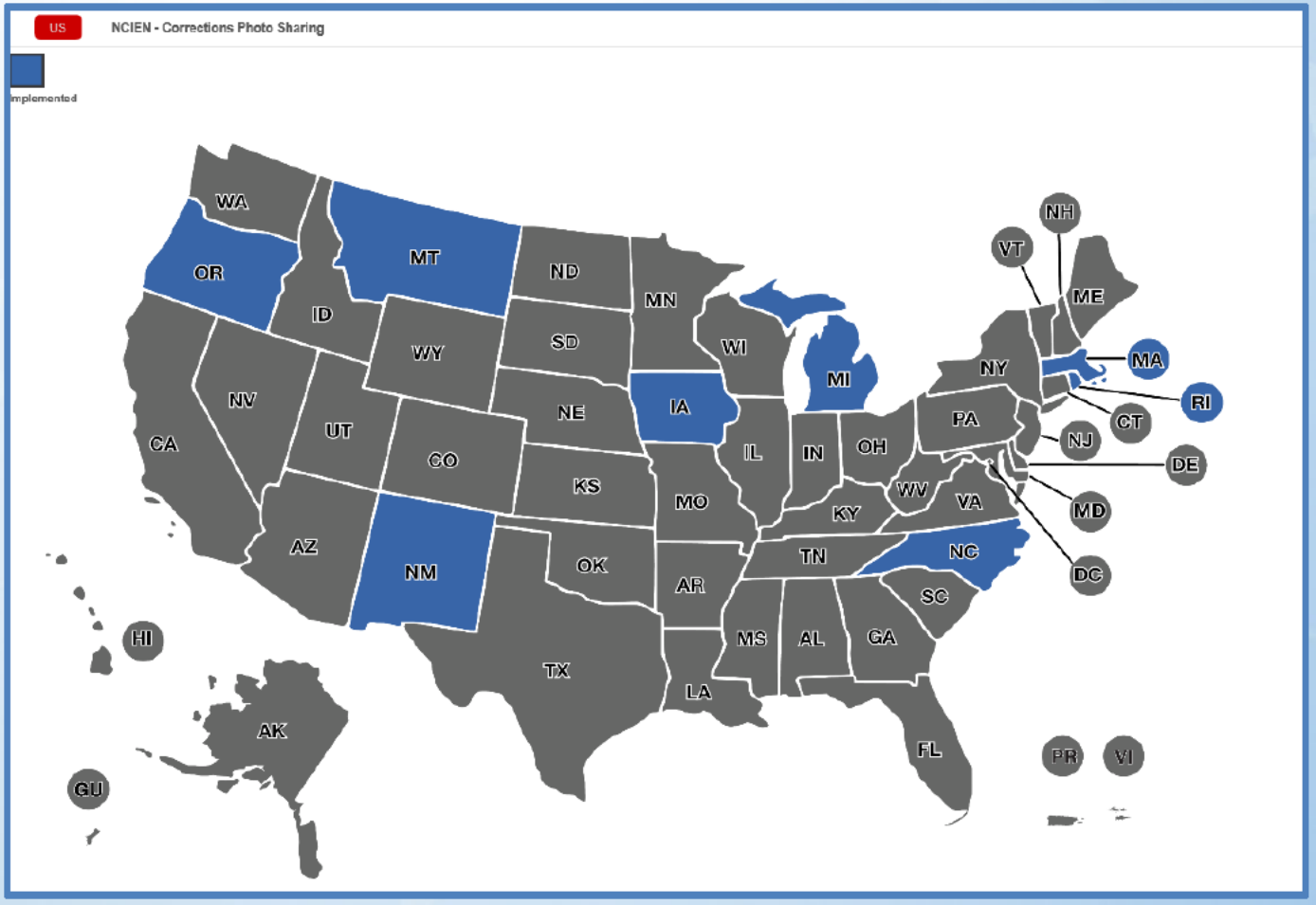


Corrections photos could include the inmates photo but also scars, marks, and tattoos, all of which will be supplemented with supervision requirements.

Access by participating states to ***previously incarcerated offenders*** and ***subjects involved in current criminal investigations*** that do not hold a driver license.





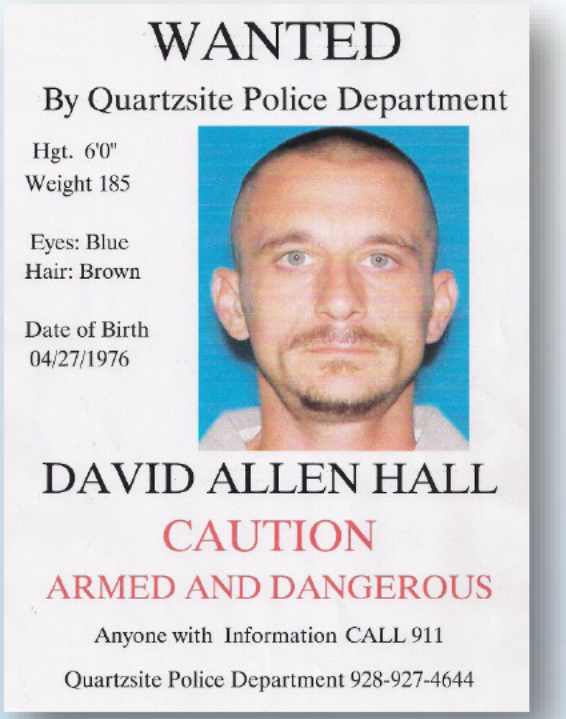

US
NCIEN - Corrections Photo Sharing
Implemented
WA
OR
CA
ID
NV
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MS
MI
IN
KY
TN
AL
OH
WV
GA
FL
SC
NC
VA
PA
NY
MD
DE
NJ
CT
RI
MA
VT
NH
ME
HI
AK
GU
PR
VI



Targeted Interstate Photo Sharing

TIPS

Powered By Nlets



The TIPS project has helped to extend image capability to include the transmission of wanted persons, missing children, vehicles, identifying scars, marks, and tattoos, and other critical images to officers on the street.

AM received by a state ***with*** image capability

AM. [redacted]
20:52 05/08/2012 26169
20:52 05/08/2012 00073 P6
TXT
* POWERED BY NLETS *

REQUEST FOR REGIONAL BROADCAST

1513 YP032 [redacted] 05/08/12
REGARDING PD [redacted] MISSING JUVENILE RUNAWAY
ATTN STATE OF GEORGIA AND SPOKANE, WA
[redacted], KAYLA NICOLE [redacted]
W/F 502/100 BLU/BRO
LSW A GRN T SHIRT AND JEANS
FEMALE LEFT A NOTE SAYING SHE WAS ENROUTE
TO SPOKANE OR GEORGIA VIA BUS TO MEET UP
WITH A BOY NAMED JOSH WHO SHE HAS BEEN
COMMUNICATING WITH GEORGIA TELEPHONE NUMBER
[redacted]
OCA [redacted]
IF FEMALE IS LOCATED CONTACT PD [redacted]
[redacted]/AFTER HRS [redacted]
THANKS
B [redacted] PD [redacted] DISPATCH
MRI 538134 IN: NLI1 29610 AT 08MAY2012 23:51
OUT: NMSC 463 AT 08MAY2012 23:51



Photo Link – Phase 2 of project



Users that can initiate an image through the NJP or their state message switch will be able to attach an image to an alert message.



Nlets will take this message, create an image cache in a file server, and provide a link to pass it through to all Nlets users allowing them to access it over the Internet.

AM received by a state ***without*** image capability

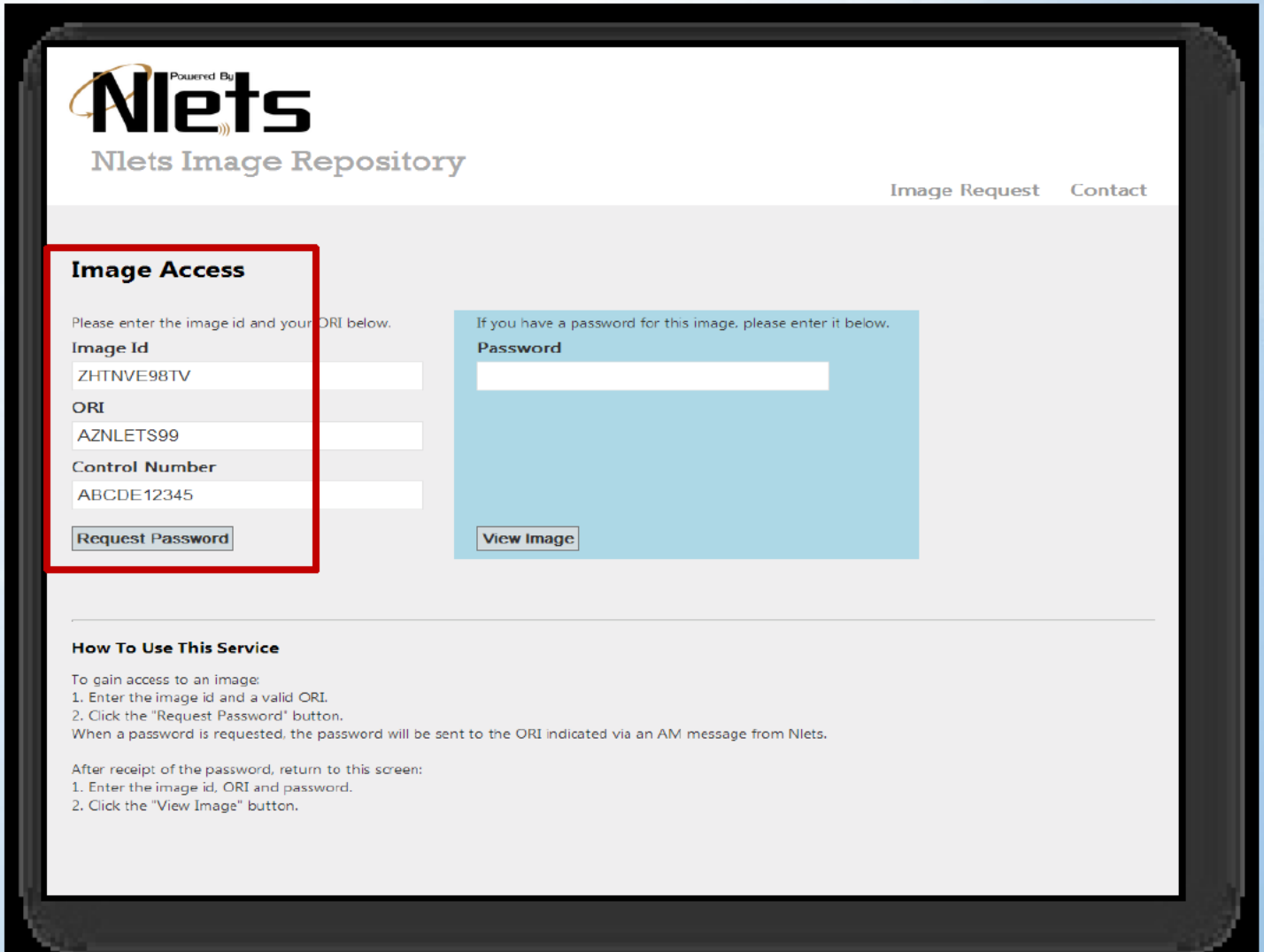
AM.AZNLETS99
14:37 05/07/2013 00001
14:37 05/07/2013 00001 AZNLETS99
*ABCDE12345

Control Number

TXT
** IMAGE **
http://images.nlets.org/TIPSImageAccesss/ZHTNVE98TV
** IMAGE **

Click the link to get to the Nlets Image Repository

Image ID

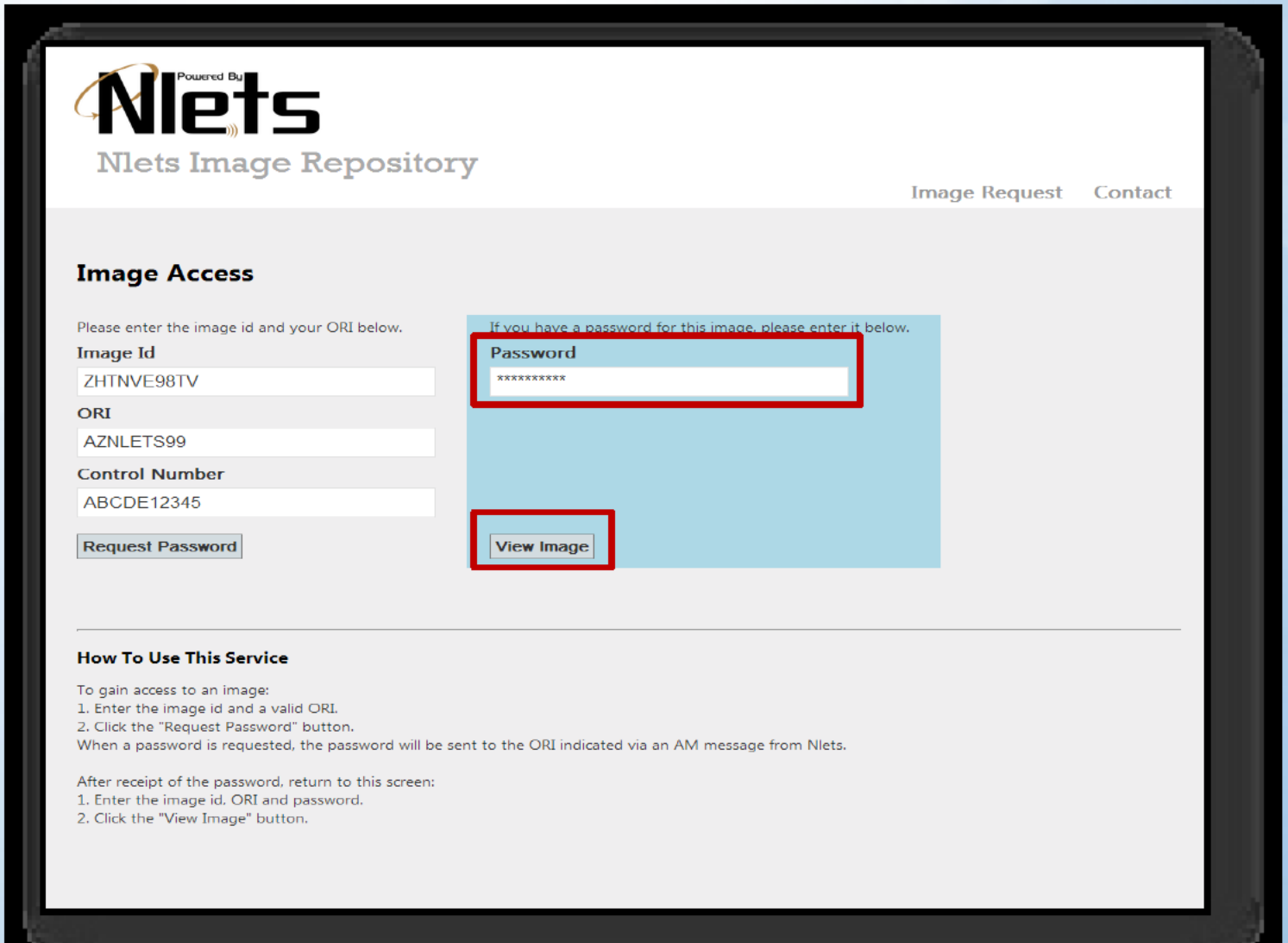

Powered By
Nlets
Nlets Image Repository
Image Request
Contact
Image Access
Please enter the image id and your ORI below.
Image Id
ZHTNVE98TV
ORI
AZNLETS99
Control Number
ABCDE12345
Request Password
If you have a password for this image, please enter it below.
Password
View Image
How To Use This Service
To gain access to an image:
1. Enter the image id and a valid ORI.
2. Click the "Request Password" button.
When a password is requested, the password will be sent to the ORI indicated via an AM message from Nlets.
After receipt of the password, return to this screen:
1. Enter the image id, ORI and password.
2. Click the "View Image" button.

AM received containing one-time use password

AM.NL0000000
14:40 05/07/2013 00007
14:40 05/07/2013 00001 AZNLETS99
*ABCDE12345
TXT
****

NLETS IMAGE REPOSITORY PASSWORD RESPONSE
****

Image URL:
http://images.nlets.org/TIPSImageAccesss/ZHTNVE98TV
Password: 8pdYp3w2$!R


Powered By
Nlets
Nlets Image Repository
Image Request
Contact
Image Access
Please enter the image id and your ORI below.
Image Id
ZHTNVE98TV
ORI
AZNLETS99
Control Number
ABCDE12345
Request Password
If you have a password for this image, please enter it below.
Password
****
View Image
How To Use This Service
To gain access to an image:
1. Enter the image id and a valid ORI.
2. Click the "Request Password" button.
When a password is requested, the password will be sent to the ORI indicated via an AM message from Nlets.
After receipt of the password, return to this screen:
1. Enter the image id, ORI and password.
2. Click the "View Image" button.

Powered By Nlets

Nlets Image Repository

Image Request Contact

Image Display

Image Key
ZHTNVE98TV

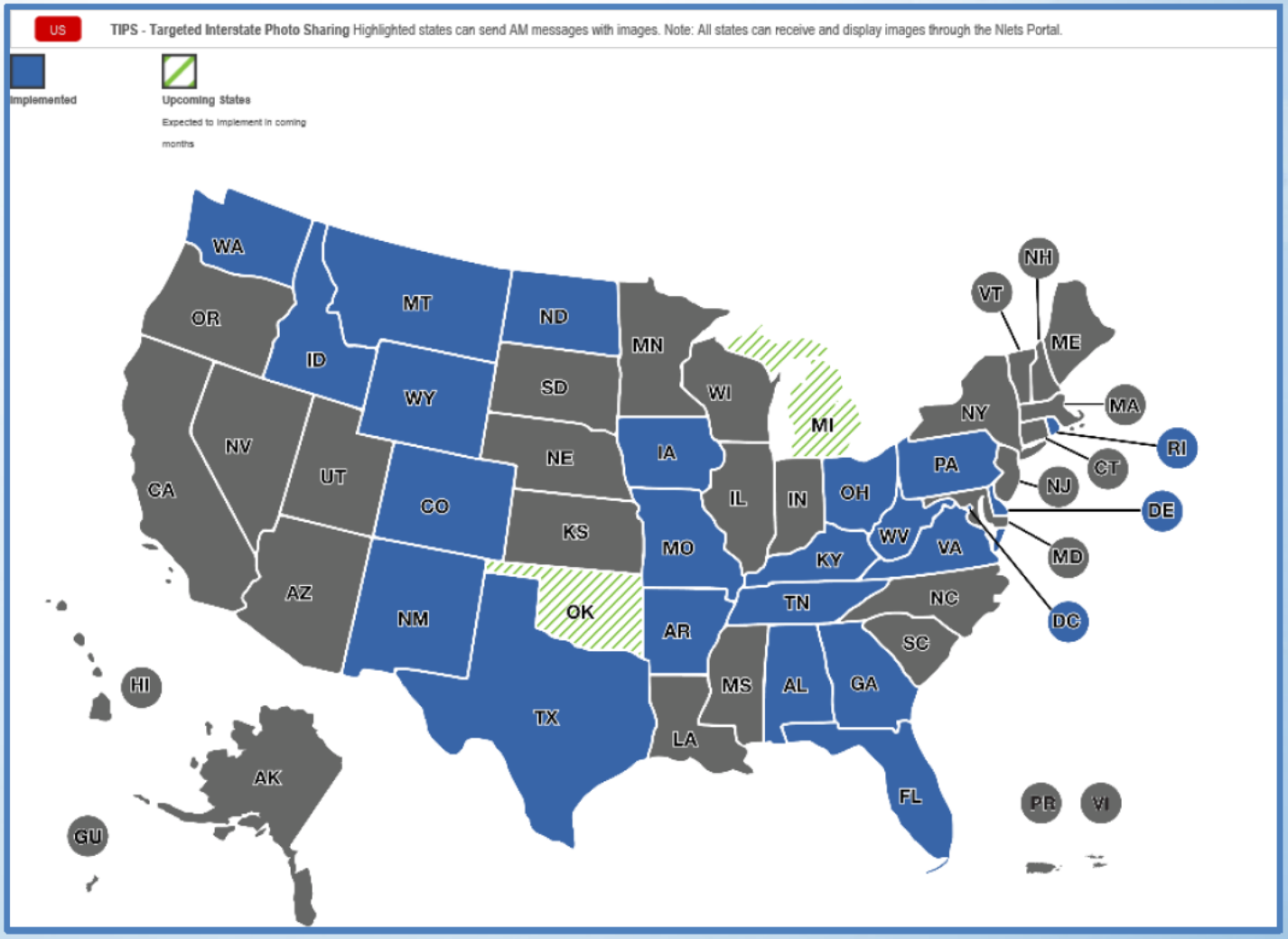
Requesting ORI
AZNLETS35

Control/Routing Number



Authorized Use Only

© 2013 - Nlets | nlets.org


US
TIPS - Targeted Interstate Photo Sharing Highlighted states can send AM messages with images. Note: All states can receive and display images through the Niets Portal.
Implemented
Upcoming States
Expected to implement in coming months
WA
OR
CA
ID
NV
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MS
MI
IN
KY
TN
AL
OH
WV
GA
FL
SC
NC
VA
PA
NY
VT
NH
ME
MA
RI
CT
NJ
DE
MD
DC
PR
VI
HI
AK
GU



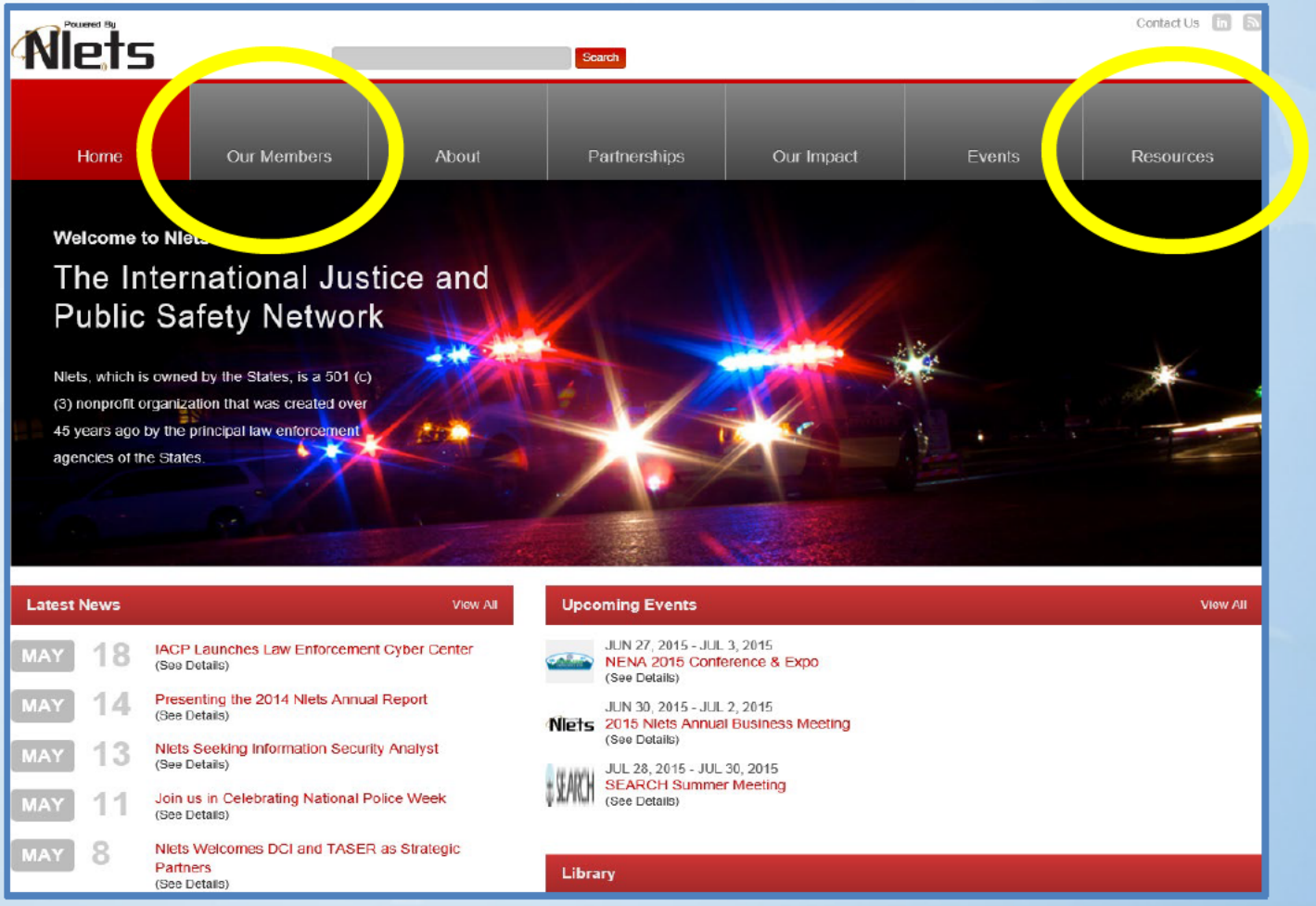
Nlets Resources

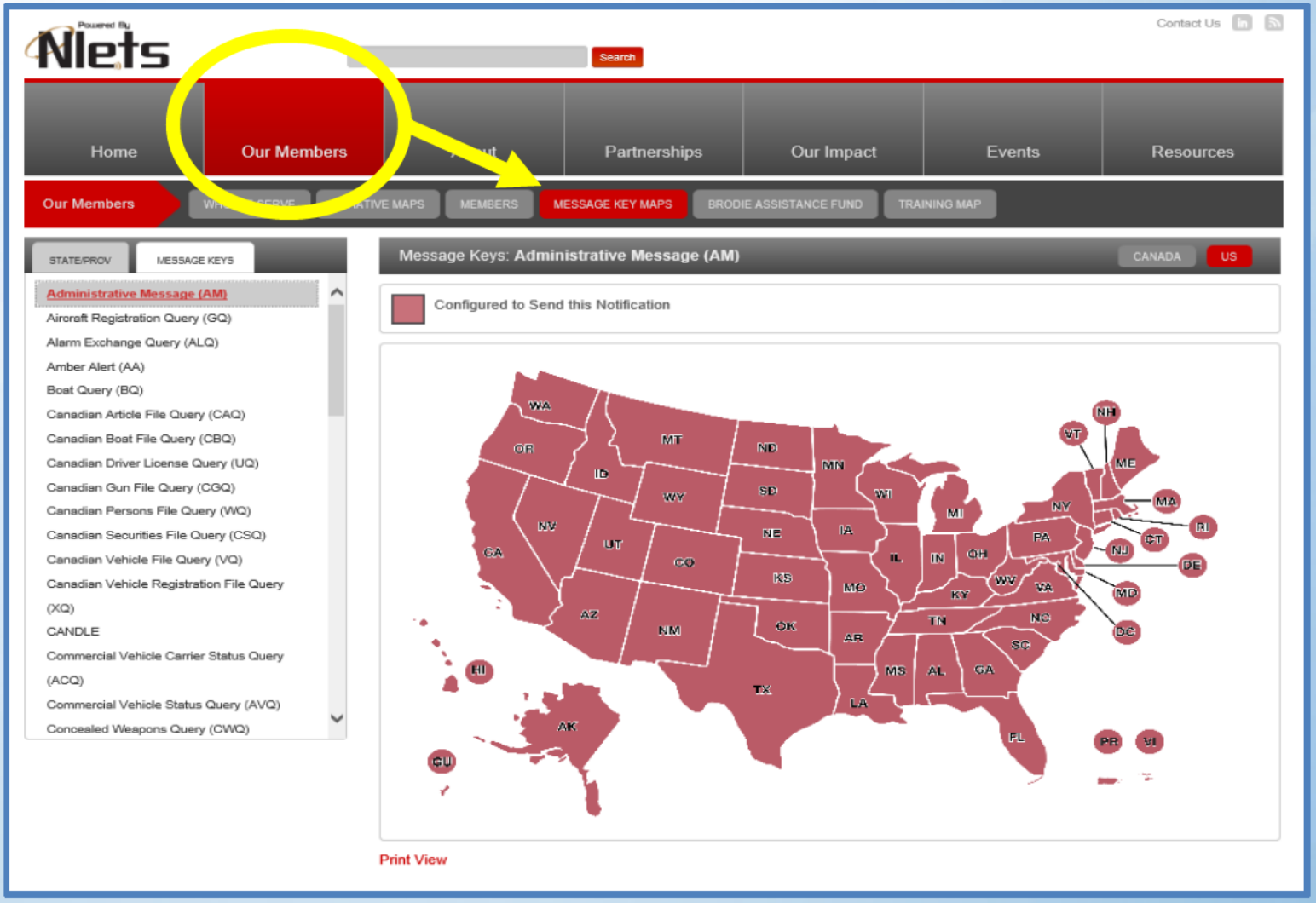


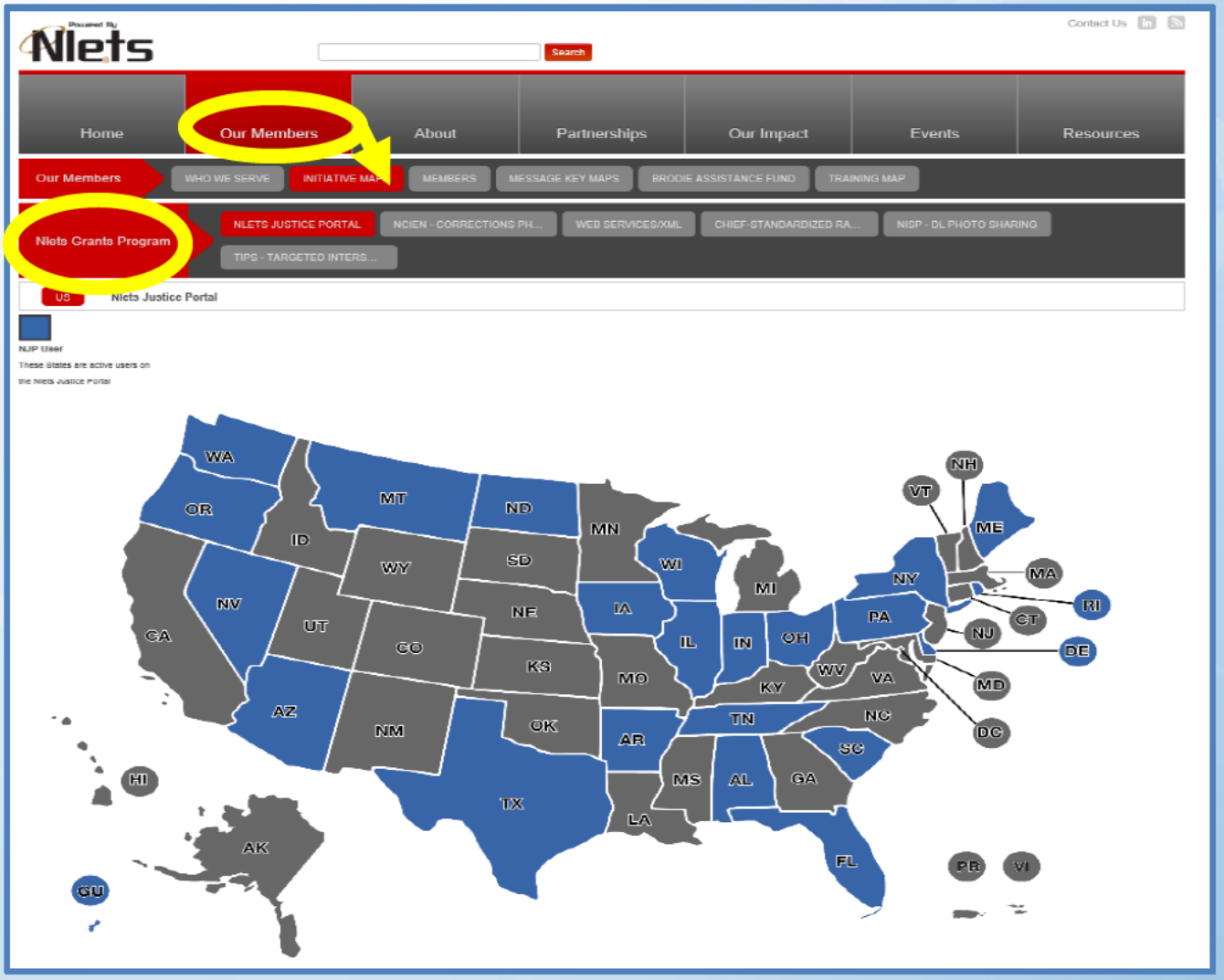
www.nlets.org

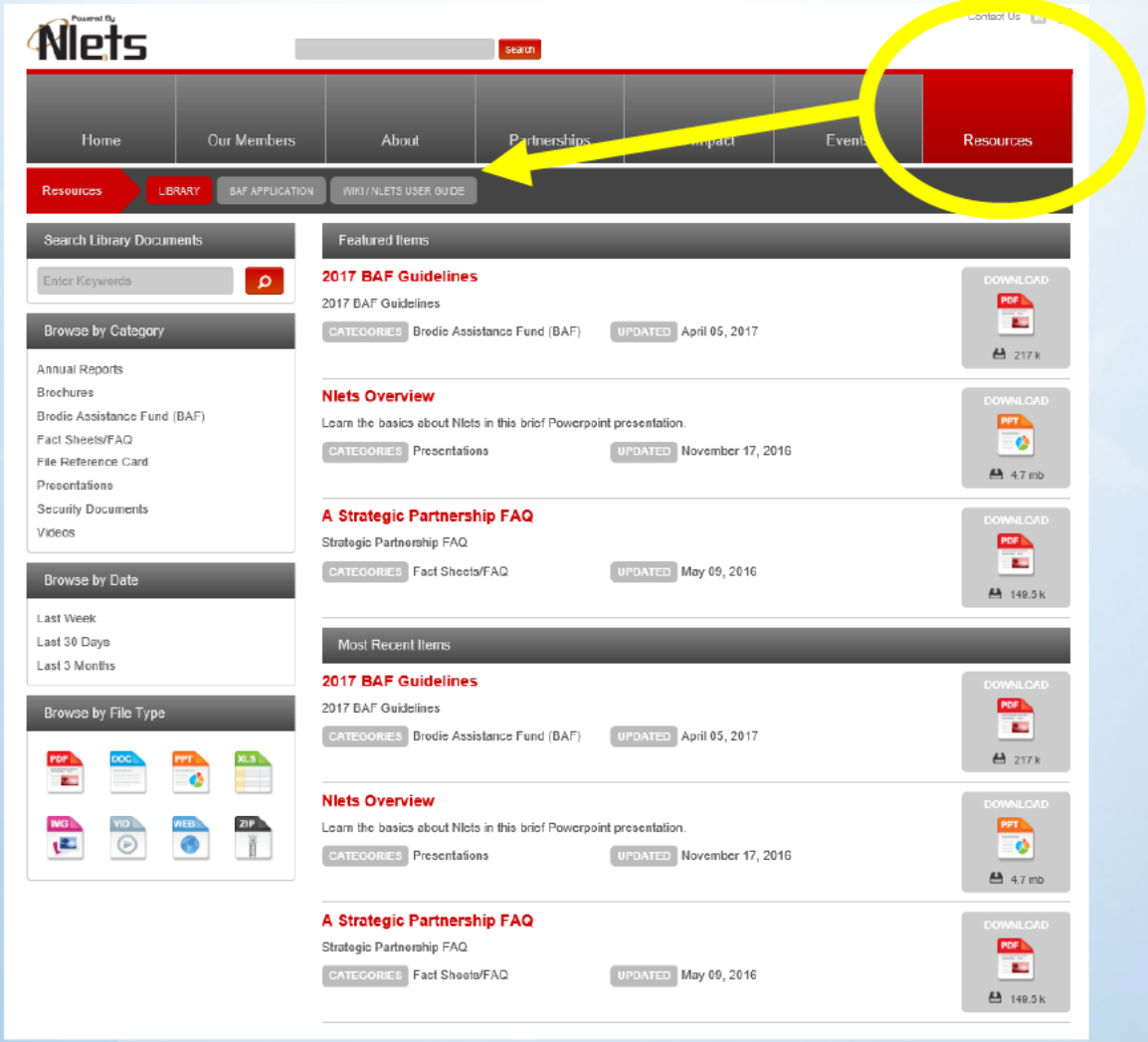
Nlets Website

Powered By Nlets

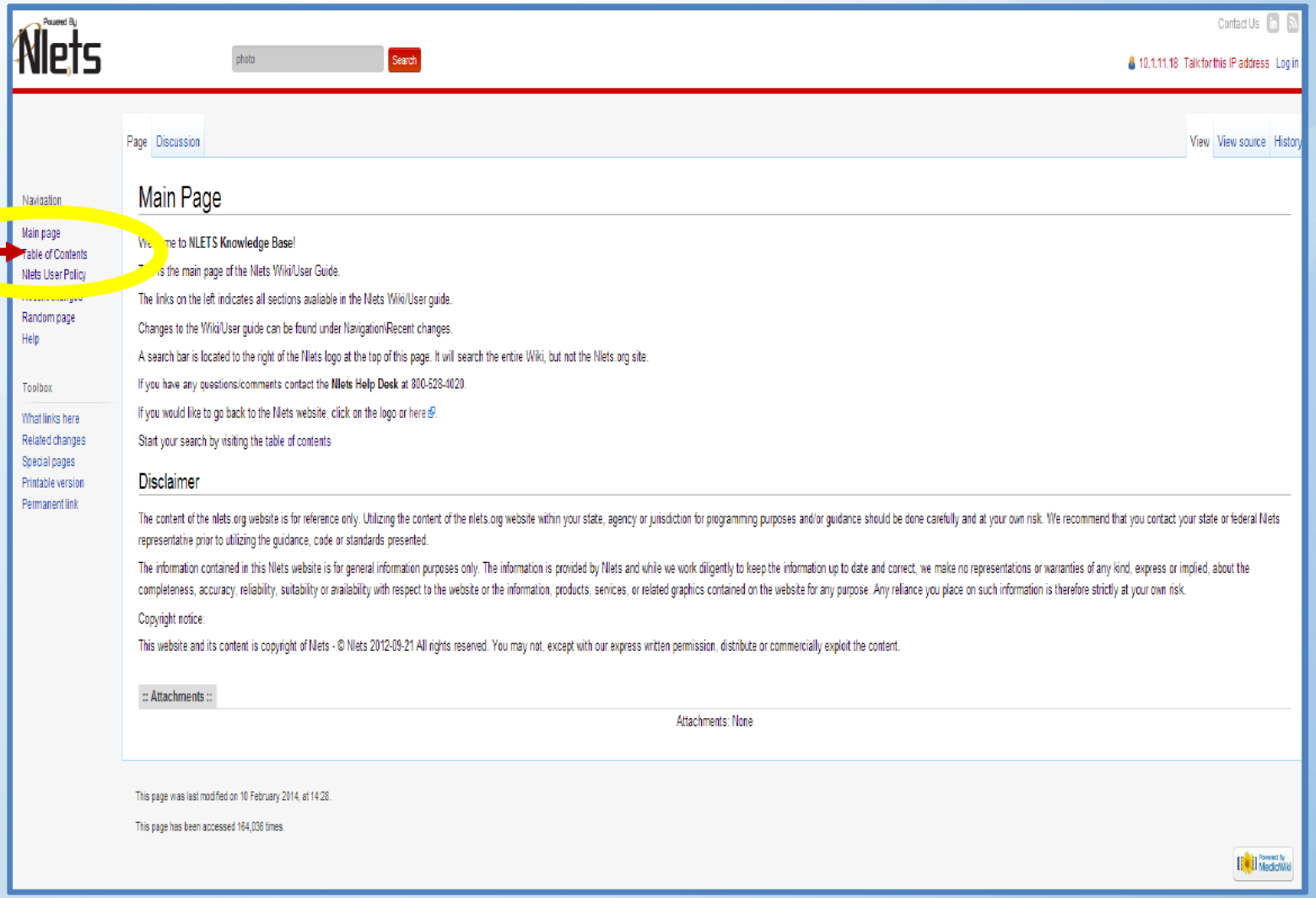

Powered By
Nlets
Contact Us
Search
Home
Our Members
About
Partnerships
Our Impact
Events
Resources
Welcome to Nlets
The International Justice and Public Safety Network
Nlets, which is owned by the States, is a 501 (c) (3) nonprofit organization that was created over 45 years ago by the principal law enforcement agencies of the States.
Latest News
View All
MAY 18 IACP Launches Law Enforcement Cyber Center (See Details)
MAY 14 Presenting the 2014 Nlets Annual Report (See Details)
MAY 13 Nlets Seeking Information Security Analyst (See Details)
MAY 11 Join us in Celebrating National Police Week (See Details)
MAY 8 Nlets Welcomes DCI and TASER as Strategic Partners (See Details)
Upcoming Events
View All
JUN 27, 2015 - JUL 3, 2015
NENA 2015 Conference & Expo
(See Details)
JUN 30, 2015 - JUL 2, 2015
2015 Nlets Annual Business Meeting
(See Details)
JUL 28, 2015 - JUL 30, 2015
SEARCH Summer Meeting
(See Details)
Library


Nlets
Search
Contact Us
Home
Our Members
Partnerships
Our Impact
Events
Resources
Our Members
MEMBERS
MESSAGE KEY MAPS
BRODIE ASSISTANCE FUND
TRAINING MAP
STATE/PROV
MESSAGE KEYS
Administrative Message (AM)
Aircraft Registration Query (GQ)
Alarm Exchange Query (ALQ)
Amber Alert (AA)
Boat Query (BQ)
Canadian Article File Query (CAQ)
Canadian Boat File Query (CBQ)
Canadian Driver License Query (UQ)
Canadian Gun File Query (CGQ)
Canadian Persons File Query (WQ)
Canadian Securities File Query (CSQ)
Canadian Vehicle File Query (VQ)
Canadian Vehicle Registration File Query (XQ)
CANDLE
Commercial Vehicle Carrier Status Query (ACQ)
Commercial Vehicle Status Query (AVQ)
Concealed Weapons Query (CWQ)
Message Keys: Administrative Message (AM)
CANADA
US
Configured to Send this Notification
WA
OR
CA
ID
NV
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MS
MI
IN
KY
TN
AL
OH
WV
GA
FL
SC
NC
VA
PA
NY
MD
DE
NJ
CT
RI
MA
VT
NH
ME
DC
PR
VI
AK
HI
GU
Print View


Powered By
Nlets
Search
Contact Us
Home
Our Members
About
Partnerships
Our Impact
Events
Resources
Our Members
WHO WE SERVE
INITIATIVE MAP
MEMBERS
MESSAGE KEY MAPS
BRODIE ASSISTANCE FUND
TRAINING MAP
Nlets Grants Program
NLETS JUSTICE PORTAL
NCIEN - CORRECTIONS PH...
WEB SERVICES/XML
CHIEF-STANDARDIZED RA...
NISP - DL PHOTO SHARING
TIPS - TARGETED INTERS...
US
Nlets Justice Portal
NJP User
These States are active users on the Nlets Justice Portal
WA
OR
CA
ID
NV
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MS
MI
IN
KY
TN
AL
OH
WV
GA
FL
SC
NC
VA
PA
NY
MD
DE
NJ
CT
RI
MA
VT
NH
ME
DC
HI
AK
GU
PR
VI



Or: wiki.nlets.org



Powered By Nlets

photo Search

Contact Us

10.1.11.18 Talk for this IP address Log in

Page Discussion View View source History

Navigation

Main page
Table of Contents
Nlets User Policy
Random page
Help

Toolbox

What links here
Related changes
Special pages
Printable version
Permanent link

Main Page

Welcome to **NLETS Knowledge Base**!

This is the main page of the Nlets Wiki/User Guide.

The links on the left indicates all sections avaliable in the Nlets Wiki/User guide.

Changes to the Wiki/User guide can be found under Navigation\Recent changes.

A search bar is located to the right of the Nlets logo at the top of this page. It will search the entire Wiki, but not the Nlets.org site.

If you have any questions/comments contact the **Nlets Help Desk** at 800-528-4020.

If you would like to go back to the Nlets website, click on the logo or here.

Start your search by visiting the table of contents

Disclaimer

The content of the nlets.org website is for reference only. Utilizing the content of the nlets.org website within your state, agency or jurisdiction for programming purposes and/or guidance should be done carefully and at your own risk. We recommend that you contact your state or federal Nlets representative prior to utilizing the guidance, code or standards presented.

The information contained in this Nlets website is for general information purposes only. The information is provided by Nlets and while we work diligently to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the website or the information, products, services, or related graphics contained on the website for any purpose. Any reliance you place on such information is therefore strictly at your own risk.

Copyright notice:

This website and its content is copyright of Nlets - © Nlets 2012-09-21 All rights reserved. You may not, except with our express written permission, distribute or commercially exploit the content.

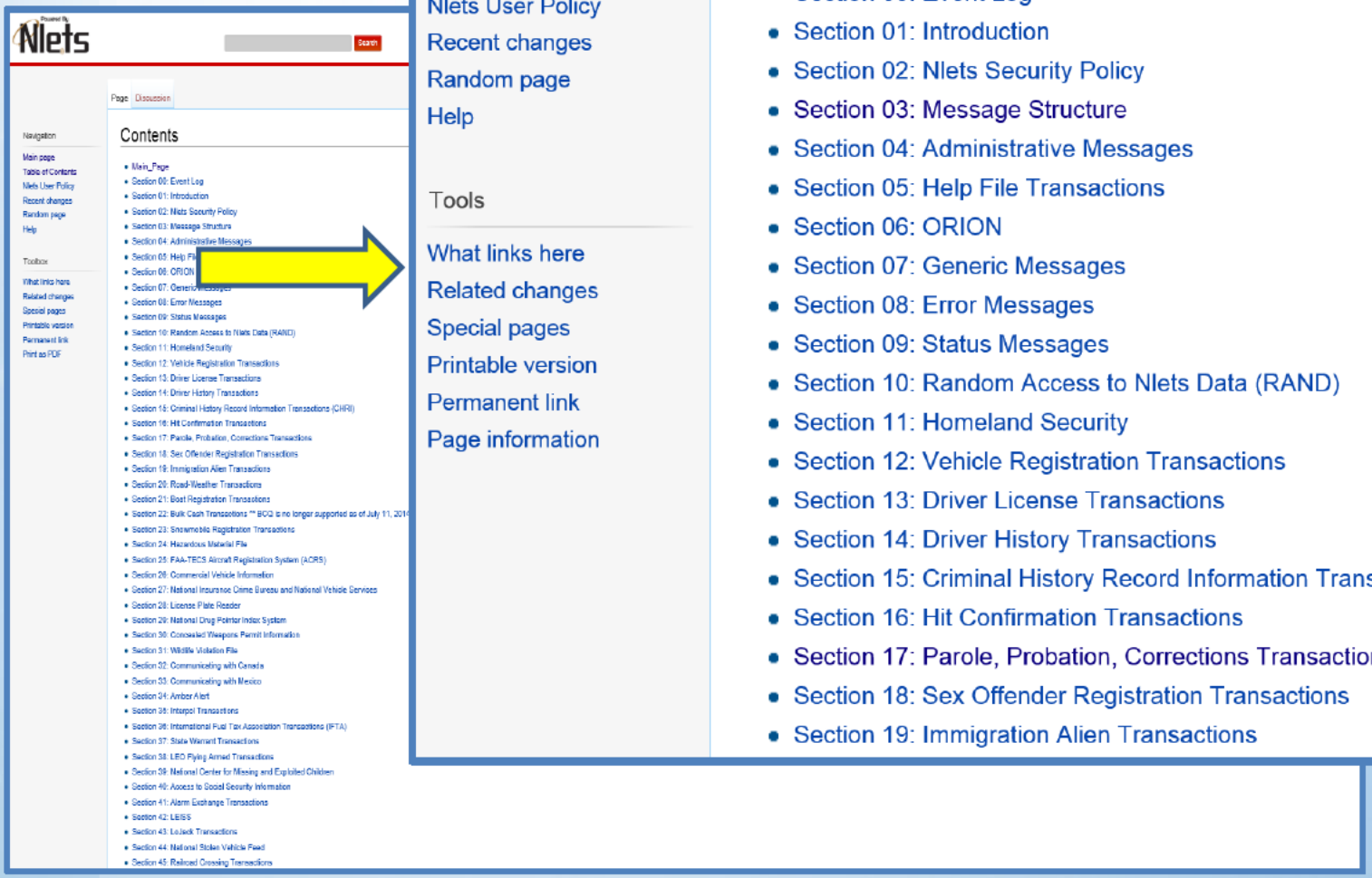
:: Attachments ::

Attachments: None

This page was last modified on 10 February 2014, at 14:28.

This page has been accessed 164,036 times.

Powered By MediaWiki



Navigation

Main page
Table of Contents
Nlets User Policy
Recent changes
Random page
Help

Tools

What links here
Related changes
Special pages
Printable version
Permanent link
Page information

Contents

- Main_Page
- Section 00: Event Log
- Section 01: Introduction
- Section 02: Nlets Security Policy
- Section 03: Message Structure
- Section 04: Administrative Messages
- Section 05: Help File Transactions
- Section 06: ORION
- Section 07: Generic Messages
- Section 08: Error Messages
- Section 09: Status Messages
- Section 10: Random Access to Nlets Data (RAND)
- Section 11: Homeland Security
- Section 12: Vehicle Registration Transactions
- Section 13: Driver License Transactions
- Section 14: Driver History Transactions
- Section 15: Criminal History Record Information Transactions (CHRI)
- Section 16: Hit Confirmation Transactions
- Section 17: Parole, Probation, Corrections Transactions
- Section 18: Sex Offender Registration Transactions
- Section 19: Immigration Alien Transactions



Listing of State Test Records

NLTSTHELP

Powered By Nlets

AM to 'NLTSTHELP'

HEADER

AM.NLTSTHELP

09:45 09/25/2017 07582

09:45 09/25/2017 00035 AZNLETS43

TXT

NLETS TEST MESSAGE FILE - NLTSTHELP

ORGANIZED ALPHABETICALLY BY STATE OR ORGANIZATION.

NOT ALL STATES SUPPORT ALL MESSAGE TYPES.

DL Test Records with an image listed at the bottom of this file.

INTERPOL Test Records with an image listed at the bottom of this file.

Alphabetical By State

AK - ALASKA

BQ:

DQ: NAM/CDL, IAMAMINOR S.DOB/19800511.SEX/M

RQ: LIC/JUNK1.LIY/2012.LIT/PC

FQ: SID/AK00999668

IQ: NAM/CDL, IAMAMINOR SAMPLE.DOB/19800511.SEX/M.SOC/000175443

IQ: NAM/CDL, IAMAMINOR SAMPLE.DOB/19800511.SEX/M.RAC/W

AZ - ARIZONA

BQ: REG/9999ZZ

DQ: NAM/OFFICE, D L.DOB/19560910.SEX/M

DQ: OLN/D00627956

RQ: VIN/1J4GW68N3XC517442

RQ: LIC/ACJ000.LIY/2009.LIT/PC

FQ: PUR/C.ATN/INVESTIGATOR SMITH.SID/AZ00000311

IQ: PUR/C.ATN/INVESTIGATOR SMITH.NAM/VADER, DARTH.DOB/19360923.SEX/M.SOC/528221487

SWQ: NAM/PUBLIC,JOHN Q.DOB/051441

SWQ: NAM/RUSTY, NAILS.OLN/B55544444

SWQ: NAM/HIGH, LENNIE.OLN/B234234234.MNU/AN-87868584

SWQ: NAM/BAD, MAN.SOC/777334444

SWQ: NAM/HUGH, LAINE.DOB/04041934

DL Test Records With An Image

AL - OLN/F034311

DE - OLN/1245293

MA - OLN/S93305014

ME - NAM/DUCK,DONALD.DOB/19901010.SEX/M

MI - NAM/DRIVER,ANNE CARR.DOB/19621120.SEX/F

MS - OLN/888888882

NC - OLN/1

NJ - OLN/P90307677852622

OH - OLN/ZZ000001

OR - OLN/1

OR - OLN/3975620

OR - OLN/1859112

PA - OLN/90000001

SD - OLN/00616775

TX - OLN/34144914

WY - OLN/109962068

INTERPOL Test Records With Image

IPQ:

NAM/Gadahn, Adam.DOB/19780901.SEX/M

FPQ:

EID/ 2004/24346



El Paso Intelligence Center

EPIC

Powered By Nlets

- Established 1974
- Support Law Enforcement Agencies
- Provide Intelligence on:
  - ✓ Drugs
  - ✓ Illegal Aliens
  - ✓ Weapons
  - ✓ Illicit Bulk Cash/Money Laundering
  - ✓ Transnational Criminal Organizations



EPIC is a multi-agency center that includes federal, state, local, tribal and foreign law enforcement agencies:





General Watch

24/7 Tactical Support

1-888-USE-EPIC (873-3742)

EPIC.general.watch@usdoj.gov

EPIC System Portal

24/7 System Access

https://esp.usdoj.gov

Request for Information

915-760-2700

request.for.information.EPIC@usdoj.gov



Nlets Secure Cloud Platform - NOVA

Powered By
Nlets Secure Cloud Platform

NOVA

- Provide a secure cloud platform for the use of law enforcement and companies that support law enforcement.
  - ***Nova is the only public cloud platform audited by the FBI CJIS Division!***
  - Nova is supporting customers with access to NJIN and the Nlets Network
- Be scalable, flexible, and robust so that services run from Nova have consistent quality and access to new features.
  - Nova is continuously upgraded and scaled (transparent to customer)
  - Nova continues to maintain high SLA's and performance
  - New features are introduced seamlessly

Tech Questions – Contact Me

Tony Abate
Nlets Sr. Systems Architect
(623) 308-3528
tabate@nlets.org



Ready to Join – Contact Me



Bonnie Locke
Nlets Director, Business Development
(623) 308-3504
newbiz@nlets.org



Curt Wood, Undersecretary
MA Executive Office of Public Safety and Security
Nlets Representative / Regional Chair
617-274-5512
curtis.wood@state.ma.us



Teri M. Fournier-Harsin
Nlets Training Manager
623-308-3552
teri@nlets.org
training@nlets.org

Questions?



3M Science. Applied to Life.™

3M Center, Bldg 225-4N-14
St. Paul, MN 55144-1000
P: 1-877-777-3571
E: 3mtssdorders@mmm.com

Quote Number	00011716	Created Date	3/22/2017
Quote Name	P492 Fixed Camera + Plate Alert Software	Expires On	6/20/2017
Prepared By	John Tedona	Contact Name	Brian Egnitz
Phone	1-201-841-6237	Email	brian.egnitz@state.ma.us
Email	jtedona@mmm.com		
Bill To Name	STATE OF MASSACHUSETTS DEPT OF STATE POLICE	Ship To Name	STATE OF MASSACHUSETTS DEPT OF STATE POLICE
Bill To	490 WORCESTER RD FRAMINGHAM, Massachusetts 01702 United States		

Quantity	Product Code	Product	Product Description	List Price	Total Price	Total S & H
[redacted]	75030254587	3M™ Plate Alert Analytics 1 YR		[redacted]	USD 12,000.00	USD 0.00
	75030254546	3M™ Plate Alert Basic 1 YR for 41-100 devices			USD 15,000.00	USD 0.00
	75030254579	3M™ Plate Alert Pattern 1 YR			USD 9,000.00	USD 0.00
	75030235792	P492 750NM 50/35 8GB W/HOOD	The 3M™ Fixed Wide Lane ALPR Camera P492 captures multiple license plates in the same field of view across 13.6 feet of US freeway traffic lanes. It is designed to utilize smaller, high power LEDs and provides the best color overview image resolution offered by 3M™ ALPR cameras.		USD 330,000.00	USD 2,250.00
		UL Listed 15V Power Supply Camera Interface Module 15V	Provides 15V power, Ethernet and RS232 connections to P392 Cameras. Designed to fit into the 3M ALPR interface boxes listed above. Bottom bracket may be removed for installation of customer provided DIN rail mounting clip for customer cabinet mounting.		USD 22,500.00	USD 0.00
	75030222303	UNIVERSAL FIXED BRKTS (P392+/P492/P382)	Accessories for ALPR fixed cameras		USD 25,500.00	USD 0.00

Total Price	USD 414,000.00
Shipping and Handling	USD 2,250.00
Grand Total	USD 416,250.00

Terms: Net 30 days
F.O.B. Freight will be prepaid by 3M and billed to customer
Shipping Costs: 3M to prepay and add to invoice
Warranty: One year return-to-depot included with purchase

Conditions of This Sale:

- Prices quote herein are firm fixed prices for your project and are valid for 90 days, unless otherwise specified.

3M Center, Bldg 225-4N-14
St. Paul, MN 55144-1000
P: 1-877-777-3571
E: 3mtssdorders@mmm.com

- Pricing is based on supplying the designated item(s) shown. Any changes in quantities or item descriptions will require new pricing to evaluate the Quotation without written consent from 3M Traffic Safety and Security Division.
- The prices quoted exclude any applicable taxes and duties, including local sales taxes
- 3M reserves the right to revise this Quotation in the event that any of the terms and conditions set forth are varied.
- An estimated delivery date range will be provide for all non-budgetary quotes. Due to resourcing requirements and the nature of the identity management business the delivery estimates are subject to change.
- Additional 3M terms and Conditions of Sales are attached

Information for PO:

- Provide your corporate Tax ID number or Tax Exempt Certificate
- 'Ship To', 'Bill To', Deliver to Contact Name and Phone Number
- Acknowledgement of shipping and handling to be added to Invoice at time of shipment and/or charge freight collect against customer's account (provide account #)

Terms and Conditions of Sale

These Terms and Conditions of Sale ("Terms") apply to every order ("Order") of products or services ("Products") by 3M Traffic Safety and Security Division ("3M"). 3M's acceptance of each Order is expressly conditioned on the Buyer's acceptance of all the Terms. If any 3M proposal is construed as an offer, that offer is expressly limited by these Terms. Any notice of different or additional terms, including, without limitation, any terms on a Buyer's purchase order, or any Buyer notice of rejection of the Terms, is hereby rejected. If any 3M action regarding a proposal from Buyer, including 3M's shipment of Products, is construed as an acceptance of Buyer's offer, such acceptance is expressly conditioned on Buyer's acceptance of these Terms.

1. Pricing and Shipping: Pricing is as provided in the 3M quotation or applicable 3M price page ("Quotation"). Prices quoted by 3M are valid for 90 days after the date of the Quotation. Any changes in quantity or release dates may result in a change in pricing. Prices are F.O.B. point of shipment and exclude shipping, taxes, and any applicable duties.

2. Payment Terms: Payment terms are net 30 days from the date of 3M invoice.

3. Credit: 3M may, in its sole discretion at any time, change or limit the amount or duration of credit extended to the Buyer. 3M may cancel any Orders or delay shipment of an Order, if the Buyer fails to meet payment schedules or other credit or financial requirements established by 3M.

4. Lead Times: Delivery lead times will be quoted at the time of Order. 3M will use reasonable efforts to ship within quoted lead times, but is not liable for delivery delays.

5. Returned Goods Policy: Returns are subject to 3M's then current Returned Goods Policy. In all instances, authorization must be received from your 3M customer service representative before any returns will be accepted.

6. Export Control Compliance: Products are delivered within the United States. The ultimate destination of any Products purchased for export or re-export must be disclosed to 3M at the time of order. Buyer is responsible for complying with all applicable export control laws.

7. Product Selection and Use: The technical information, recommendations and other statements relating to the Products are based upon tests or experience that 3M believes are reliable, but the accuracy or completeness of such information is not guaranteed. Many factors beyond 3M's control and uniquely within Buyer's knowledge and control can affect the use and performance of a Product in a particular application Given the variety of factors that can affect the use and performance of a Product, Buyer is solely responsible for evaluating the 3M product and determining whether it is fit for a particular purpose and suitable for Buyer's method of application.

8. Confidentiality: Any information supplied by 3M in response to Buyer's request for quotation will not be used for any purpose other than to evaluate 3M's proposal and, except as required by law, may be not be disclosed or used for any other purpose.

9. Warranty and Limited Remedy: THE FOLLOWING IS MADE IN LIEU OF ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. 3M warrants that its 3M Security Systems Division products will meet 3M's written specifications at the time of shipment. 3M's obligation and your exclusive remedy shall be, at 3M's option, to replace or repair the 3M product or refund the purchase price of the 3M product. IN NO EVENT WILL 3M BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES INCLUDING, BUT NOT LIMITED TO LOSS OF PROFITS, IN ANY WAY RELATED TO THE PRODUCTS REGARDLESS OF THE LEGAL THEORY ASSERTED.

10. Federal Contracts: 3M is selling commercial items as defined in FAR 2.101. If an Order is issued under a Federal Government contract or higher-tier subcontract, the following additional terms and conditions apply to the extent that the terms and conditions are applicable based on their FAR or DFARS prescriptions for commercial item procurements, as of the date of the Order: FAR 52.212-5(e) when the buyer's government contract is for commercial items or services, FAR 52.244-6 when the buyer's government contract is for noncommercial items/services, and additionally, DFARS 252.212-7001(c) when the buyer's contract is with the Department of Defense.

The FAR and DFARS specify that for the acquisition of commercial items, prime contractors (Buyer) are not required to flow down any FAR clauses other than those listed above. Therefore, acceptance of any order placed by Buyer does not constitute acceptance by 3M of any other government contract provision other than those listed above, regardless of terms and conditions included on Buyer boilerplate order documents, and any such provisions are expressly rejected as a condition of these Terms.

3M Center, Bldg 225-4N-14
St. Paul, MN 55144-1000
P: 1-877-777-3571
E: 3mtssdorders@mmm.com

11. Changes: 3M reserves the right to amend, modify, or supplement these Terms as to future orders or shipments. No action by Buyer may amend, modify, reject, supplement, or waive these Terms in any manner whatsoever (including course of dealing or of performance or usage of trade) except as agreed upon in a writing signed by an authorized representative of 3M.

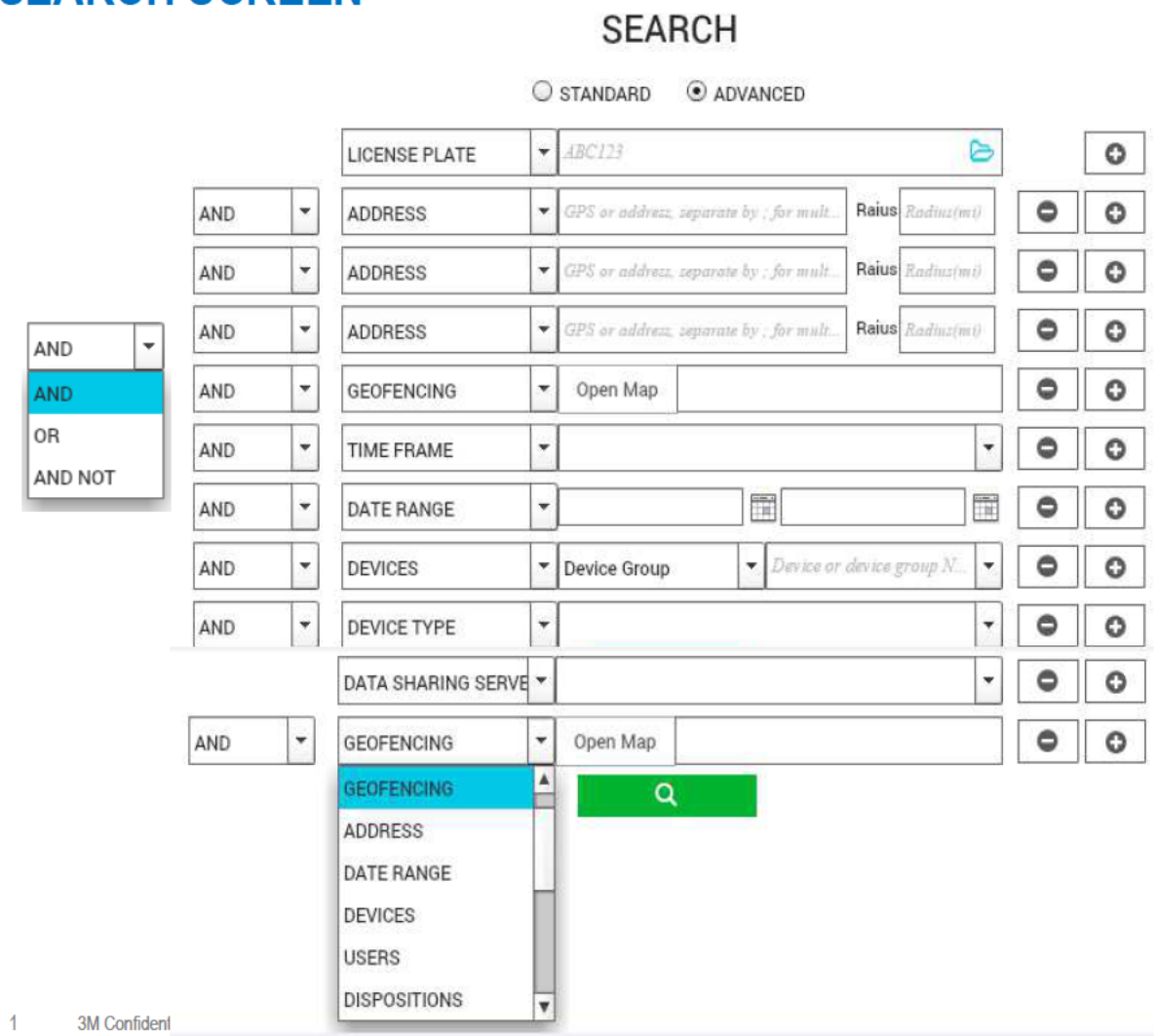
12. Waiver: Any failure or delay by either Party in exercising any right or remedy provided by or relating to the Quotation or these Terms in one or more instances does not constitute a waiver and shall not prohibit a Party from exercising such right or remedy at a later time or from exercising any other right or remedy available.

13. Severability: If any provision of the Quotation or these Terms shall, for any reason, be held invalid, illegal, or unenforceable by a court or tribunal of competent jurisdiction, such provision shall be deemed severable and such invalidity, illegality, or unenforceability shall not affect any other provision of the Quotation or these Terms which shall be enforced in accordance with the intent of this Agreement.

14. Complete Agreement: The Quotation and these Terms constitute the entire agreement between the Parties and supersede and terminate any and all prior agreements and understandings, whether written or oral, between the Parties with respect to the subject matter of the Order. Each Party agrees that it has not relied on any representation, warranty, or provision not expressly stated herein and that no oral statement has been made to either Party in any way tends to waive any of the these terms. The UN Convention on the International Sale of Goods shall not apply.

US SGBG TSSD ALPR Direct

SEARCH SCREEN



NEW FEATUERS

- Multi-Address
- Geo-Fencing
- Enhanced Auditing/Reporting
- Cruising Patterns
- Short Duration Patterns
- Convoy Patterns
- Cohort Patterns
- Cloned Plates
- “Portal” Across non-3M ALPR
- PA-to-PA or PA-to BOSS
  - ➢ In/Out

© 3M 2016. All Rights Reserved.

3M Science. Applied to Life.™

NEW! 3M™ Plate Alert Analytical ALPR Software

The Confidence to act.



Next-generation ALPR software uses data fusion analytics and proactive alerts to give you more answers and the confidence to act.

New 3M™ Plate Alert Analytical ALPR Software goes beyond ALPR — to deliver near-real time intelligence that extends officers' reach.

ALPR has long been an important tool for law enforcement — even though sorting and analyzing long lists of plate reads can be a tedious and time-consuming task.

But what if you could merge all that information from ALPR with other sources to automatically uncover relevant connections, spot patterns, and issue alerts — in near-real time?

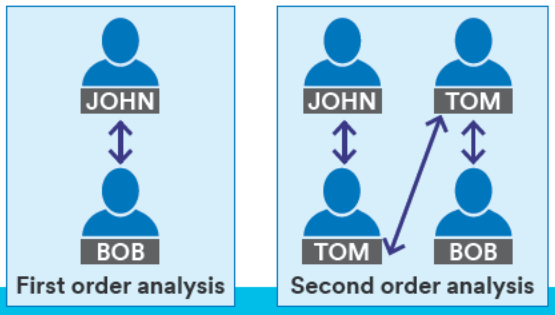


Making ALPR data work harder

3M™ Plate Alert Analytical ALPR Software goes beyond conventional ALPR to deliver actionable intelligence that you can't get from other systems.

The program is designed to be fast, powerful, and intuitive ALPR software. But that's just the beginning.

Plate Alert software can compile ALPR data with data from various sources, such as 911 calls, pawn data, police reports, motor vehicle data and more. It can then almost instantly find connections between data points to deliver solid, meaningful leads — in a fraction of the time, and with more accuracy — than a human analyst.



3M™ Plate Alert Analytical ALPR Software is the first ALPR software powered by data fusion analytics. Using sophisticated second-order analysis, data fusion analytics deliver more answers and more actionable intelligence than conventional ALPR software that relies on first-order analysis.

Data Fusion Analytics

What is Data Fusion?

Data fusion integrates diverse data into a single, unified view to create a more complete, informative, accurate, and useful picture. By linking and simultaneously evaluating numerous common characteristics across multiple data sources, it can uncover unexpected relationships and associations. In practice, it can uncover relevant connections and provide a clear view of how seemingly unrelated people, places, things and events are connected, and how they impact each other. This means you can get more answers from your data, and you can get leads you can't get from other systems.

Benefits

- ☑ More useful, actionable leads
- ☑ Save personnel time spent collecting, organizing, and analyzing data
- ☑ Help avoid missing critical information which can get buried in mountains of data
- ☑ Greater accuracy and confidence in results

Data Sources

The more data sources that are fused together, the better the insight. Data fusion analytics harness ALPR data and then fuse it with other available data sources to deliver in-depth situational awareness. Some examples of data sources that ALPR can be fused with are:

- 911 calls
- Fire incidents and related inspection records
- Pedestrian and vehicle investigation reports
- Intelligence feeds
  e.g., DHS / HSIN alerts, BOLOs, Amber Alerts, Wanted Felons, Sex Offender Registry, etc.
- Pawn data
- SARS (Suspicious Activity Reports)
- CAD/RMS (Incident and Arrest records)
- CBRNE (Chemical, Biological, Radiological, Nuclear and Explosive) data, alarms and reports

Pattern Management Alerts

What are Pattern Management Alerts?

They automatically push notifications of activity to users, helping them take action faster. Notifications are sent when the system detects activity that matches a pre-defined pattern, and alerts proactively provide relevant information so almost all the work is done before someone even looks at the data.

Going beyond typical ALPR software which just alerts when a plate read matches a watch list, Pattern Management sends alerts of patterns which may suggest illicit activity. For example, a “911 to LPR” alert provides license plates which are captured within the vicinity of a 911 call. The user can configure the 911 incident types, the window of time and distance surrounding the 911 call, and the devices to be included.

Pattern management alerts are easily configured, enabled, or disabled. Each alert contains multiple filters and parameters to fine-tune to user needs.

Benefits

- ☑ Proactively deliver actionable insights
- ☑ Help you take action faster with near real-time delivery
- ☑ Pre-populated alerts are easy to setup and enable
- ☑ Almost all the work is done before someone even looks at the data

Plate Alert is pre-populated with three categories of patterns:



Vehicle patterns

Some patterns use ALPR data on its own, such as Cloned Plate which detects and alerts on a single license plate captured at two locations within an impossibly short time. Other patterns use other data sources, such as 911 call data, to tie a vehicle to an event.



People patterns

Leveraging reports, records, and pawn data, people can be tied to events. For example, the Burglar Arrest Pawner alert is triggered if a pawner has a burglary-related arrest record.



Item patterns

Checking items against serial number, make, model, or description, these alerts tie items to events. For example, Burglary to Pawn (Serial Number) uses an item’s serial number to check whether a stolen item has been pawned.

Six ways 3M™ Plate Alert Analytical ALPR Software can help you work smarter



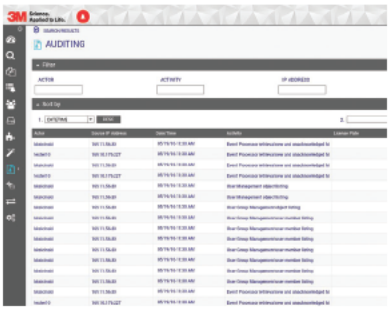
Make your ALPR data work harder

Perform standard and advanced ALPR searches, discover and act on patterns of activity, and easily create detailed, visual reports.



Turn data into confident decisions

Plate Alert software uses advanced data fusion analytics to continuously analyze conditions across multiple sources to give you a clear view of how seemingly unrelated people, places, things and events are connected. The result? More actionable leads than a long list of plate reads.



Improve data privacy

Multiple data privacy measures include auditing, customizable user permissions and multiple data controls, for precise customization.



Take action faster

Pattern alerts proactively deliver actionable insights in near-real time, helping you take action faster.



Less time clicking

We collaborated with human factors scientists to make 3M™ Plate Alert Analytical ALPR Software easy to learn and to search, get alerts, find leads and take action.



See the big picture

Quickly assess results with easily understood visual displays, mapping and visualization tools such as scatterplots.

	Feature	3M BOSS	3M Plate Alert
Alert List (Hotlist) Management	Alert List Display	Only displays alert lists in a list format	Displays alert lists in a list or tile format
	Delete, Enable & Disable Alert Lists	Drill down into alert list screen to delete/enable/disable alert list	Allows delete and enable/disable, for one or more alert lists, on the main Alert List Management screen
	Alert List Group	Not available	Control behavior, deployment, and notification of alert lists at group level
	Formatting	Requires complex formatters to be created by 3M to use on alert lists	Allows the user to create the formatting based on the file via the wizard
	Alert List Field Name and Order	Dependent on the source file; cannot be changed by the users	Allows for customizing the name of each field and the order it appears in an alert
	Location List	Has quick hotlist Location list (e.g. CA DOJ Felony, TX DPS Stolen)	Not available; location list is based on format, and Plate Alert software doesn't allow for this formatting
	Alert Frequency	Allows for per-minute polling, or polling every one to 24 hours	Allows for scheduling an alert list from every hour to once a month and everything in between
	Send Alert to Other Agency	Allows for sending remote alerts to another agency	Not Available
	Alert List Assignment on Device	Assign alert lists among devices	Assign alert lists among devices
	Alert List Management by User	Control which user(s) will receive the alert	Control which user(s) will receive the alert
	Alert List Status and History	Display the current status of the alert lists and the updating of the source file	Display the current status of the alert lists and the updating of the source file, and the history of all the changes and source updates
Device Management	Device Display	Only displays devices in a list format	Displays devices in a list or tile format
	Delete, Enable & Disable Devices	Need to click through to device screen	Allows delete and enable/disable, for one or more devices, on the main Device Management screen
	Device Group	Supports a hierarchical view of devices within the site; allow creating "remote site" in which the devices can be viewed by data sharing agencies	Allows managing notification and data retention of devices in a group at group level
	Device Management by User	Not available	In device management, allows the control of which user(s) can view the data from a device
	Fixed Camera Location	Displays the location of a fixed camera on a map	Displays the location of a fixed camera on a map
	Device Status and History	Displays the last time a given device sent data to the system	The same as BOSS, as well as a history of statuses and changes of a device
System Parameters	User Login History	Only shows currently logged in users	Shows currently logged in users and provides a history of the login/logout times
	Disposition Priority	Allows the users to set a priority and back-office-only setting for dispositions	Allows the users to set a priority only
	Attribute Format	Attributes require database knowledge to use effectively	Lays out attributes in a user-friendly format
	Individual User Report	Allows access to reports down to the individual user level	Allows access to either all the report or none of the report
	Peer-to-Peer Sharing	Allows peer-to-peer sharing (with great difficulty)	Features an easy format for linking peer-to-peer, and control of inbound and outbound data sharing
Additional Features	Analytics	Not available	Allows a user to tie in other database systems and query those databases with the LPR data
		Not available	Draws links between data and datasets using algorithms to determine the strength of the association
	Pattern	Not available	Evaluates data in near real time to determine patterns within the data; these patterns are configurable by the user
		Not available	Pattern management can include other linked databases to find patterns
	Auditing	User requires database knowledge to create auditing reports	Allows a user to search the audit table for data without running a report
		Not available	Allows a user to configure the amount of shared data that is coming in and going out of a system; they control the age of the data and how many records per query
		Not available	Displays a history of all transactions between shared systems
	Configuration	Not available	Allows a user to configure which mapping service they wish to use
		Not available	Allows an administrator to determine the strength of a password and how frequently it must change
		Not available	Allows for global data retention settings and can purge all transaction data with one button
		Not available	Allows an administrator to configure auditing, how long to keep the audits, and what specifically will be audited

Why You Should Switch to 3M™ Plate Alert Analytical ALPR Software

With a host of features designed to maximize law enforcement effectiveness, 3M Plate Alert software is the future of ALPR back office software. When compared to 3M's past offering, 3M Plate Alert software presents a new level of flexibility in alert list management, data analytics, and inter-agency data sharing (should you choose) – all presented with a quick and intuitive user interface. The following table outlines the differences between 3M™ Back Office System Software (BOSS) and 3M Plate Alert software:

	Feature	3M BOSS	3M Plate Alert
Header, Menu Bar, and Dashboard	Menu	Options appear within three main menu items, which may require multiple clicks to find the desired information.	All menu items are available in a single layer, minimizing the clicks it takes to find information
	Day/Night Modes	Not available	Allows the user to toggle visual modes for better screen visibility and less distraction at night
	User Setting	Allows an admin to change settings such as password, email, alert timeout, alert medium, language, PAGIS/LPCS password, and the image height.	Increased user personalization, including how data is displayed in the management screens and search results, contact information, user image, and dashboard items and widgets
	Site Search	Has site search capability, but requires the user to select what part he or she wants to look for (e.g. reads, users, groups)	Site search is open text and will search against the entire site
	Dashboard	Displays read/hit/misread counts	Displays read/hit/misread counts, like BOSS. In addition, displays events and alerts counts on a map; provides widgets for the users. The dashboard is configurable and designed to allow for additional dashboard items and widgets to be added later
	Widgets	Not available	A range of configurable widgets are available, including badge icon, emails from the system, weather, office bulletin, and 3M communication
Read/Event Searching	Search Parameter	Displays all criteria at once and utilizes open text and drop down menus	Breaks the searching into two groups: standard, for quick searches of time and plate; and advanced, which allows the user to customize search using a range of parameters
	Search Result Display	Displays results in a list form by default. No tile view exists and plotting on a map requires the user to select all the data and click a map button	Allows the user to set a default for displaying the results; user can select from list view, tile view, and map view. User can toggle between these views without rerunning the search
	Search Parameter	Limited	Allows for polygon searching, multiple addresses, and/or/not logic, and a large number of parameter combinations
	Saved Search	Saved Search only displays the name of the search and does not provide the user with the criteria until after the search is executed	Displays the criteria prior to executing the search, allowing the user to decide which search will meet his or her needs.
	Multiple Searches	Allows multiple search tabs	Allows multiple search tabs
	Results Per Page	Limits the number of results per page and warns users if their search results exceed a certain number	Does not have any limitations on returned results; utilizes "lazy loading" to optimize system efficiency
	Read Detail	Limited to timestamp, device, location, site, images and GPS	Presents same content as 3M BOSS, plus all of the camera information, including vehicle travel direction, device type, and data source
Dispatch	Dispatch	View reads coming into the system in real time with details, images, and camera information	A dashboard widget displays the reads as they come in on a map but with limited details
Reports	Canned Reports	Ten canned reports	One canned report – event detail report, including images and all details around the event
	Favorite Report	Not available	Allows you to save report parameters as favorites
	Report Export	Display the report within the application and allows exporting to Excel, PDF, and Word	Loads the report in PDF
	Report Generation	Requires the system to pause when it generates a report	Does not prevent a user from using the system while it generates a report
	Report History	Not available	Shows the count of reports being generated
User Management	User Display	Displays users in a list format	Displays users in a list or tile format
	Delete, Enable & Disable Users	Allows admins to delete, enable, and disable users at user screen	Allows admins to delete enable, and disable – for one or more users – on the main User Management screen, rather than on each individual user screen
	User Group	User group is designed for roles, LPCS security and data sharing security	User group is designed for roles, LPCS security, data security and allow the management at user group level
	Terminate User Session from Management	Requires admin to go to session screen to terminate a user's session	Allows for ending a user's session from the Management screen
	User Profile and Preference	Not available	Allows resetting password, changing user profile images, device notification, setting UI default, and selecting dashboard items and notification types
	User Administration	Allows admin to set up login name, display name, group, password, email address, notification type, language preference, login expiration, and LPCS password	Allows same functions as 3M BOSS, as well as viewing GPS data, age of data, and session history
	User Login History	Not available	Shows login/logout history, including timestamp, duration, and IP address



3M gives you more ways to make faster, better-informed and safer decisions.

To provide the best security, you need the best intelligence. That's why, in addition to 3M™ Plate Alert Analytical ALPR Software, 3M offers a broad portfolio of solutions designed to help you solve more crimes, close more cases and stay a step ahead of emerging threats. These include ALPR systems, license plate technologies, vehicle information systems, electronic offender monitoring and biometric identity management solutions. They are all part of 3M's continuing commitment to support the mission of law enforcement agencies around the world.

For more information, visit www.3M.com/PlateAlert or contact the 3M customer contact center at 1-877-777-3571.

Traffic Safety and Security Division
3M Center, Building 225-4N-14
P.O. Box 33225
St. Paul MN 55133-3225
www.3M.com/PlateAlert

3M is a trademark of 3M.
Used under license in Canada.
Please recycle. Printed in USA
© 3M 2016. All rights reserved.

MMARS DOCUMENT ID: **ISAEPSJG16HEROPOL18A**

COMMONWEALTH OF MASSACHUSETTS
INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM

This Form is issued and published by the Office of the Comptroller (CTR) pursuant to 815 CMR 6.00 for use by all Commonwealth Departments. Departments may add non-conflicting additional terms, but changes to the official printed language of this Form shall be void.

BUDGET FISCAL YEAR: 2018	RFR REFERENCE NUMBER ENTER RFR NUMBER: OR __X__ N/A.
MMARS ALPHA *BUYER/PARENT* DEPARTMENT CODE: EPS	MMARS ALPHA *SELLER/CHILD* DEPARTMENT CODE: POL
BUSINESS MAILING ADDRESS: 10 PARK PLAZA, SUITE 3720 BOSTON, MA 02116	BUSINESS MAILING ADDRESS: MASSACHUSETTS DEPARTMENT OF STATE POLICE 470 WORCESTER ROAD FRAMINGHAM, MA 01702
ISA MANAGER: PAUL GARRITY	ISA MANAGER: MARIBEL FOURNIER
PHONE: **617-725-3322** FAX: 617-725-0260	PHONE: **508-820-2300** FAX: 508-820-2359
E-MAIL ADDRESS: PAUL.GARRITY@STATE.MA.US	E-MAIL ADDRESS: MARIBEL.FOURNIER@MASSMAIL.STATE.MA.US

Purpose of ISA: (Check one option only and complete applicable information) (Attachment A required for New ISAs and all ISA Amendments.)

__X__ New ISA. Current Maximum Obligation for total duration of ISA $ 97,946.80 (Use "N/A" for Non-Financial ISA.) (Complete Attachment B)

____ Amendment to Existing ISA. What is being amended? (Attachment C required for all Federal and Bond Account Amendments)

- ____ Amend Budget/Accounts. Change Maximum Obligation from: $_____ to New Maximum Obligation $_____ (Attachment B)
- ____ Amend Budget/Accounts. No Change in Maximum Obligation (Attachment B)
- ____ Amend Dates of Performance. New Dates of Service: Start Date:_____End Date:_____(Subject to execution dates below.)
- ____ Amend Scope of Services/Performance

BRIEF DESCRIPTION OF PERFORMANCE GOALS TO BE ACCOMPLISHED BY ISA, OR IF AMENDMENT, IDENTIFY WHAT IS BEING AMENDED: TO FUND THE HEROIN AND OPIOID PROGRAM

WILL SELLER/CHILD DEPARTMENT STATE EMPLOYEES (AA OBJECT CLASS) BE FULLY OR PARTIALLY FUNDED UNDER THIS ISA? **__X__ No ____ Yes.** If Yes, Seller/Child certifies that the ISA is not being used as an alternative funding mechanism for state employees, that the identified personnel in Attachment A are necessary for completion of the ISA due to particular expertise or other factors that can not be obtained through the use of contractors, and that if federal funds are being used, funds shall not be used to supplement the regular salary or compensation of any officer or employee of the Commonwealth for services performed during their regular working hours. M.G.L. c. 29, § 6B.

ACCOUNT INFORMATION. Complete for all new ISAs and Amendments (even if account information is not changing) Check one option, indicate "add", "delete" or "no change" and enter account, fund, major program code and program code.

__x__ BGCN – non-subsidiarized (federal, capital, trust). Attachment C required for any new ISA or ISA Amendment involving federal funds.
____ BGCS – subsidiarized (budgetary)
____ Other (CT, RPO as authorized by CTR): _____.
____ Non-Financial ISA (no funds are transferred from Buyer/Parent to Seller/Child), however, resources are committed to ISA.
____ Amendment with no Accounting Changes to Budget/Accounts or to Attachments B or C. (Indicate no change below and complete account information.)

__X__ ADD __ DELETE __ NO CHANGE	Account:80004611	Fund: 0100	Major Program Code: BJAG	Program Code: FJG1HEOP16
__ ADD __ DELETE __ NO CHANGE	Account:	Fund:	Major Program Code:	Program Code:
__ ADD __ DELETE __ NO CHANGE	Account:	Fund:	Major Program Code:	Program Code:
__ ADD __ DELETE __ NO CHANGE	Account:	Fund:	Major Program Code:	Program Code:

ISA ANTICIPATED START DATE: **12/01/2017** provided that the Seller/Child certifies that it will not incur any obligations related to this ISA prior to the date that this ISA is executed, NOR prior to the date that sufficient funding for the obligations for this ISA is available in the Seller/Child account for expenditure.

TERMINATION DATE OF THIS ISA: This ISA shall terminate on **11/30/2018** unless terminated or properly amended in writing by the parties prior to this date.

BUYER/PARENT AND SELLER/CHILD DEPARTMENT CERTIFICATIONS. IN WITNESS WHEROF, by executing this ISA below, the Buyer/Parent and Seller/Child certify, under the pains and penalties of perjury, that Buyer/Parent and Seller/Child understand and agree that any Buyer/Parent or Seller/Child officer or employee who knowingly violates, authorizes or directs another officer or employee to violate any provision of state finance law relating to the incurring of liability or expenditure of public funds, includng this ISA, may be considered to be in violation of M.G.L. c. 29, § 66, and therefore the Buyer/Parent and the Seller/Child agree to ensure that this ISA complies with, and that all staff or contractors involved with ISA performance are provided with sufficient training and oversight to ensure compliance with 815 CMR 6.00, CTR applicable policies and the ISA Terms and Conditions which are incorporated by reference into this ISA, in addition to the performance requirements identified in Attachnent A of this ISA, and that all terms governing performance of this ISA are attached to this ISA or incorporated by reference herein, and the Buyer/Parent and Seller/Child agree to maintain the necessary level of communication (including immediate notification of any amendments to accounting information, program codes or performance needs), coordination, access to reports and other ISA information, and cooperation to ensure the timely execution and successful completion of the ISA, amendments, and state finance law compliance; and that the Buyer/Parent certifies it will ensure that sufficient funds are timely made available in the Seller/Child account(s), with the proper accounting codes, prior to the Seller/Child's need to begin initial or amended performance; and that the Seller/Child will not allow initial or amended performance to begin until the ISA is executed AND the ISA Seller/Child account is sufficiently funded to support encumbrances and payments for performance (including payroll), and the Seller/Child will make encumbrances and payments (including payroll) only from the authorized ISA Seller/Child account(s) and shall not be entitled to transfer charges made from any other account not approved in writing by CTR in advance of expenditures by the Seller/Child.

20BUYER/PARENT DEPARTMENT'S AUTHORIZED SIGNATURE: **DATE:** (Date must be handwritten by signatory at time of signature)	**SELLER/CHILD DEPARTMENT'S AUTHORIZED SIGNATURE:** **DATE:** (Date must be handwritten by signatory at time of signature)
PRINT NAME: ANGELA F. F. DAVIS	PRINT NAME:
PRINT TITLE: EXECUTIVE DIRECTOR	PRINT TITLE:

ISAEPSJG16HEROPOL18A

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM

TERMS AND CONDITIONS

The following terms and conditions are incorporated by reference into any ISA.

Role of the Office of the Comptroller. All ISA fiscal transactions shall be made through the state accounting system as prescribed by the Office of the Comptroller (CTR). CTR will interpret 815 CMR 6.00 and applicable policies and take any fiscal or other actions necessary to ensure ISA compliance with state finance law, including but not limited to correcting accounting transactions, resolving ISA disputes and identifying corrective action by the Buyer/Parent or Seller/Child Departments.

Seller/Child Department Certifications. By executing an ISA the Seller/Child certifies that it is statutorily authorized to provide the type of performance sought by the Buyer/Parent, and shall at all times remain qualified to perform the ISA, that performance shall be timely and meet or exceed ISA standards, that the Seller/Child will not allow initial or amended performance to begin, may not authorize personnel or contractors to work, nor incur any obligation to be funded under an ISA prior to the execution of an ISA AND the availability of ISA funding in the Seller/Child account to support encumbrances and payments for performance. The Seller/Child will make encumbrances and payments (incuding payroll) only from the authorized ISA Seller/Child account(s) and shall not be entitled to transfer charges made from any other account not approved in writing in advance by CTR. The Seller/Child must immediately notify CTR whenever a delay in funding is anticipated for which performance is expected. The Seller/Child is authorized to use ISA funding only for the actual costs of ISA performance and may not use ISA funds to supplement non-ISA related personnel or expenditures.

Buyer/Parent Department Certifications. Signature by the Buyer/Parent certifies that it is statutorily authorized or required to procure the type of performance required under this ISA, that the Buyer/Parent certifies it will ensure that sufficient funds are timely made available in the Seller/Child Seller/Child account(s), with the proper accounting codes, prior to the Seller/Child's need to begin intial or amended performance; that the Buyer/Parent will monitor and reconcile ISA performance in compliance with state appropriation language or federal grant requirements, communicate all fiscal information necessary for the set up of the Seller/Child account(s) including budget information, and if the ISA is funded with federal funds provide accurate accounting information in Attachment C, and immediately notify the Seller/Child of any changes in Attachment C (such as program codes) to ensure the ISA and Seller/Child account can be timely updated to avoid lapses in funding or the inability of the Seller/Child to make timely payroll and other expenditures from the Seller/Child account.

Chief Fiscal Officer. The Chief Fiscal Officer (CFO) for the Buyer/Parent and Seller/Child will be responsible for the fiscal management of ISAs within their Departments in accordance with these ISA Terms and Conditions, 815 CMR 6.00 and policies and procedures published by CTR.

ISA Manager. Both the Buyer/Parent and Seller/Childs are responsible for ensuring that the ISA Manager listed on the ISA, or ISA Amendment, is current and that the ISA Manager is an authorized signatory for the Department supported by the appropriate Security Profile. If the listed ISA Manager changes, the CFO shall be the ISA Manager until a replacement is identified in the same manner as other Written Notice.

Record-keeping and Retention, Inspection of Records. The Buyer/Parent and Seller/Child shall maintain all ISA records in such detail as necessary to support claims for payment, including reimbursement or federal financial participation (FFP), for at least seven (7) years from the last payment under an ISA Seller/Child account, or such longer period as is necessary for the resolution of any litigation, claim, negotiation, audit or other inquiry involving an ISA. In addition to any specific progress, programmatic or expenditure reports specified in Attachment A, the Seller/Child is required to provide the Buyer/Parent (and to CTR, the State Auditor and the House and Senate Ways and Means Committees upon request) with full cooperation and access to all ISA information.

Payments and Compensation. The Seller/Child may accept compensation only for performance delivered and accepted by the Buyer/Parent in accordance with the specific terms and conditions of the ISA. All ISA payments are subject to appropriation pursuant to M.G.L. C. 29, or the availability of sufficient non-appropriated funds for the purposes of an ISA. Overpayments or disallowed expenditures shall be reimbursed by the Seller/Child or may be offset from future ISA payments in accordance with state finance law and instructions from CTR.

ISA Termination or Suspension. An ISA shall terminate on the date specified, unless this date is properly amended prior to this date, or unless terminated or suspended under this Section upon prior written notice to the Seller/Child. The Buyer/Parent may terminate an ISA without cause and without penalty with at least thirty days prior written notice, or may terminate or suspend an ISA with reasonable notice if the Seller/Child breaches any material term or condition or fails to perform or fulfill any material obligation required by an ISA, or in the event of an elimination of an appropriation or availability of sufficient funds for the purposes of an ISA, or in the event of an unforeseen public emergency mandating immediate Buyer/Parent action. Upon immediate notification to the other party, neither the Buyer/Parent nor the Seller/Child shall be deemed to be in breach for failure or delay in performance due to Acts of God or other causes factually beyond their control and without their fault or negligence. Contractor failure to perform or price increases due to market fluctuations or product availability will not be deemed factually beyond the Seller/Child's control.

Written Notice. Any notice shall be deemed delivered and received when submitted in writing in person or when delivered by any other appropriate method evidencing actual receipt by the Buyer/Parent or the Seller/Child. Unless otherwise specified in the ISA, legal notice sent or received by the Buyer/Parent's ISA Manager or the CFO (with confirmation of actual receipt) through the listed fax number(s) or E-Mail address for the ISA Manager will satisfy written notice under the ISA. Any written notice of termination or suspension delivered to the Seller/Child shall state the effective date and period of the notice, the reasons for the termination or suspension, if applicable, any alleged breach or failure to perform, a reasonable period to cure any alleged breach or failure to perform, if applicable, and any instructions or restrictions concerning allowable activities, costs or expenditures by the Seller/Child during the notice period.

Confidentiality. The Seller/Child shall comply with M.G.L. C. 66A if the Seller/Child becomes a "holder" of "personal data". The Seller/Child shall also protect the physical security and restrict any access to personal or other Buyer/Parent data in the Seller/Child's possession, or used by the Seller/Child in the performance of an ISA, which shall include, but is not limited to the Buyer/Parent's public records, documents, files, software, equipment or systems. If the Seller/Child is provided access with any other data or information that triggers confidentiality requirements under FIPA, HIPPA or other federal or state laws, the Seller/Child shall be responsible for protection of this data as instructed by the Buyer/Parent.

Assignment. The Seller/Child may not assign, delegate or transfer in whole or in part any ISA, or any liability, responsibility, obligation, duty or interest under an ISA, to another Department or an outside contractor. Assumption of an ISA by a successor Department due to a legislative change in the Seller/Child or Buyer/Parent's department status shall be accomplished through the execution of a new ISA.

Subcontracting By Seller/Child. Since it is presumed that contracting through the Seller/Child is more cost effective and a better value than the Buyer/Parent directly contracting with an outside contractor(s), any subcontract entered into by the Seller/Child for the purposes of fulfilling the obligations under an ISA must be approved by the Buyer/Parent in advance of the ISA and justified as part of the ISA Attachment A. The Seller/Child is responsible for full state finance law and procurement compliance for all subcontracts, and shall supply a copy of any subcontract to the Buyer/Parent upon request.

Affirmative Action, Non-Discrimination in Hiring and Employment. In performing this ISA, the Seller/Child shall comply with all federal and state laws, rules, regulations and applicable internal state policies and agreements promoting fair employment practices or prohibiting employment discrimination and unfair labor practices and shall not discriminate in the hiring of any applicant for employment nor shall any qualified employee be demoted, discharged or otherwise subject to discrimination in the tenure, position, promotional opportunities, wages, benefits or terms and conditions of their employment because of race, color, national origin, ancestry, age, sex, religion, disability, handicap, sexual orientation or for exercising any rights afforded by law. The Seller/Child commits to, when possible, to purchasing supplies and services from certified minority or women-owned businesses, small businesses or businesses owned by socially or economically disadvantaged persons or persons with disabilities in accordance with the Commonwealth's Affirmative Market Program.

Waivers. Forbearance, indulgence or acceptance by the Seller/Child or Buyer/Parent of any breach or default in any form shall not be construed as a waiver and shall not limit enforcement remedies or allow a waiver of any subsequent default or breach.

Risk of Loss. The Seller/Child shall bear the risk of loss for any materials, deliverables, personal or other data that is in the possession of the Seller/Child or used by the Seller/Child in the performance of an ISA until is accepted by the Buyer/Parent.

Disputes. The Buyer/Parent and Seller/Child agree to take all necessary actions to resolve any dispute arising under the ISA within 30 calendar days including department head and secretariat involvement, but in no event shall a dispute remain unresolved beyond May 30th in any fiscal year, nor may the Buyer/Parent or Seller/Child allow a dispute to create a state finance law or other violation of ISA terms (such as a delay in funding, failure to timely communicate funding or program code changes, or failure to timely process ISA paperwork). Seller/Child and Buyer/Parent must immediately notify CTR to assist in resolution of the dispute and shall implement any actions required by CTR to resolve the dispute, which shall be considered final.

Interpretation, Severability, Conflicts with Law, Integration. Any amendment or attachment to any ISA that contains conflicting language or has the affect of deleting, replacing or modifying any printed language of the ISA shall be interpreted as superseded by the ISA Form as published. If any ISA provision is superseded by state or federal law or regulation, in whole or in part, then both parties shall be relieved of all obligations under that provision to the extent necessary to comply with the superseding law, provided however, that the remaining provisions of the ISA, or portions thereof, shall be enforced to the fullest extent permitted by law. The terms of this ISA shall survive its termination for the purpose of resolving any claim, dispute or other action, or for effectuating any negotiated representations and warranties.

ISAEPSJG16HEROPOL18A

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM

TERMS AND CONDITIONS

ATTACHMENT A – TERMS OF PERFORMANCE AND JUSTIFICATIONS:

This Attachment Form must be used. Insert (type or copy and paste) all relevant information using as many pages as necessary. Attach any additional supporting documentation as appropriate. If Amending the ISA, completion of Sections 1, 2 and 3 identifying what is being amended and the reasons for the amendments is required. For sections 4-9 enter only the amended language in the sections being amended.

1. [REQUIRED] Purpose and other performance goals of ISA, or as amended:

To combat the opioid epidemic, the Massachusetts State Police created a fifth division, called the Division of Homeland Security and Preparedness (referred to herein as DHS) and tasked it with spearheading the state's opioid interdiction efforts. This project will support this mission with the purchase of Automated License Plate Readers (ALPR), which can be used for suspect specific opioid distribution and trafficking investigations. Additional equipment will be purchased to exploit the telephonic communications made by opioid distributors and traffickers.

2. [REQUIRED] Identify in detail, the responsibilities of the parties, the scope of services and terms of performance under the ISA, or as amended:

- Captain Robert Sojka will be the project manager and will oversee the procurement (Goal 1) and deployment of the equipment (Goal 2), and will prepare all required reports.
- MSP Fiscal Section will oversee the financial reporting requirements and compliance
- To combat the opioid epidemic, the Massachusetts State Police created a fifth division, called the Division of Homeland Security and Preparedness (referred to herein as DHS) and tasked it with spearheading the state's opioid interdiction efforts. This project will support this mission with the purchase of Automated License Plate Readers (ALPR), which can be used for suspect specific opioid distribution and trafficking investigations. Additional equipment will be purchased to exploit the telephonic communications made by opioid distributors and traffickers.

3. [REQUIRED] Identify schedule of performance or completion dates or other benchmarks for performance, or as amended:

The anticipated start date of the ISA is on or about 12/01/2017 and the end date of the ISA is 11/30/2018**.**

4. [REQUIRED] Justification that use of ISA is best value vs. contract with outside vendor:

The seller's proposal was deemed a best value purchase based on their capacity and ability to deliver the proposed services in a professional, timely and efficient manner.

5. Will Seller/Child department state employees (AA Object Class) be fully or partially funded under this ISA? __X__ No
Yes. If Yes, justify necessity to use state employees for the ISA vs. use of contractors (contract employees or outside vendors).

6. Subcontractors. Since it is presumed that contracting through the Seller/Child is more cost effective and a better value than the Buyer/Parent directly contracting with an outside contractor(s), any subcontract entered into by the Seller/Child for the purposes of fulfilling the obligations under an ISA must be approved by the Buyer/Parent in advance of the ISA and justified as part of the ISA Attachment A, as follows: (enter "N/A" if subcontractors will not be funded with ISA funds)

N/A

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM

TERMS AND CONDITIONS

7. Identify any equipment that will be leased or purchased by the Seller/Child using ISA funds: (The Buyer/Parent shall determine ownership of equipment purchased by the Seller/Child with ISA funds. Enter "N/A" if equipment not included in ISA.)

Equipment\Technology	Description or Computation
(6) 3M Fixed Wide Lane ALPR Cameras P492	The 3M™ Fixed Wide Lane ALPR Camera P492 captures multiple license plates in the same field of view across 13.6 feet of US freeway traffic lanes.
(6) P492/P382 INTERNAL CHASSIS 48V for new Tbox	Accessories for ALPR cameras
(6) UNIVERSAL FIXED BRKTS (P392+/P492/P382)	Accessories for ALPR cameras
(6) Cradlepoint Router for Verizon Network	Accessories for ALPR cameras
Equipment Shipping costs	
(6) Hoffman UU504030 Enclosures for ALPR Cameras	Housings for ALPR cameras
(10) HP Prodesk computers with mouse and keyboard	Computers for exploitation of telecommunications
(20) HP Monitors	Monitors for above-referenced computers
(10) Microsoft Office licenses	Software for above-referenced computers

If equipment will be purchased with federal funds, please complete Attachment B to reflect the obligation for this purchase. Additionally, the seller must adhere to the federal guidelines for equipment purchased with federal grant funds included in this section.

Federal Guidelines on Equipment

The following are the guidelines on equipment found in the Federal Uniform Administrative Requirements for Grants document. As the name implies, these guidelines apply to all federal grant programs. While previously referred to as Federal OMB Circular A-102, it is now codified by each of the OGR federal granting agencies within various sections of the Code of Federal Regulations. The sections on equipment are as follows:

(a) *Title.* Subject to the obligations and conditions set forth in this section, title to equipment acquired under a grant or subgrant will vest upon acquisition in the grantee or subgrantee respectively.

(b) *States.* A State will use, manage, and dispose of equipment acquired under a grant by the State in accordance with State laws and procedures. Other grantees and subgrantees will follow paragraphs (c) through (e) of this section.

(Massachusetts State Government procedures can be found in the next section)

(c) *Use.* (1) Equipment shall be used by the grantee or subgrantee in the program or project for which it was acquired as long as needed, whether or not the project or program continues to be supported by Federal funds. When no longer needed for the original program or project, the equipment may be used in other activities currently or previously supported by a Federal agency.

(2) The grantee or subgrantee shall also make equipment available for use on other projects or programs currently or previously supported by the Federal Government, providing such use will not interfere with the work on the projects or program for which it was originally acquired. First preference for other use shall be given to other programs or projects supported by the awarding agency. User fees should be considered if appropriate.

(3) Notwithstanding the encouragement in §18.25(a) to earn program income, the grantee or subgrantee must not use equipment acquired with grant funds to provide services for a fee to compete unfairly with private companies that provide equivalent services, unless specifically permitted or contemplated by Federal statute.

(4) When acquiring replacement equipment, the grantee or subgrantee may use the equipment to be replaced as a trade-in or sell the property and use the proceeds to offset the cost of the replacement property, subject to the approval of the awarding agency.

(d) *Management requirements.* Procedures for managing equipment (including replacement equipment), whether acquired in whole or in part with grant funds, until disposition takes place will, as a minimum, meet the following requirements:

(1) Property records must be maintained that include a description of the property, a serial number or other identification number, the source of property, who holds title, the acquisition date, and cost of the property, percentage of Federal participation in the cost of the property, the location, use and condition of the property, and any ultimate disposition data including the date of disposal and sale price of the property.

(2) A physical inventory of the property must be taken and the results reconciled with the property records at least once every two years.

(3) A control system must be developed to ensure adequate safeguards to prevent loss, damage, or theft of the property. Any loss, damage, or theft shall be investigated.

(4) Adequate maintenance procedures must be developed to keep the property in good condition.

(5) If the grantee or subgrantee is authorized or required to sell the property, proper sales procedures must be established to ensure the highest possible return.

(e) *Disposition.* When original or replacement equipment acquired under a grant or subgrant is no longer needed for the original project or program or for other activities currently or previously supported by a Federal agency, disposition of the equipment will be made as follows:

(1) Items of equipment with a current per-unit fair market value of less than $5,000 may be retained, sold or otherwise disposed of with no further obligation to the awarding agency.

(2) Items of equipment with a current per unit fair market value in excess of $5,000 may be retained or sold and the awarding agency shall have a right to an amount calculated by multiplying the current market value or proceeds from sale by the awarding agency's share of the equipment.

(3) In cases where a grantee or subgrantee fails to take appropriate disposition actions, the awarding agency may direct the grantee or subgrantee to take excess and disposition actions.

(f) *Federal equipment.* In the event a grantee or subgrantee is provided federally-owned equipment:

(1) Title will remain vested in the Federal Government.

(2) Grantees or subgrantees will manage the equipment in accordance with Federal agency rules and procedures, and submit an annual inventory listing.

(3) When the equipment is no longer needed, the grantee or subgrantee will request disposition instructions from the Federal agency.

(g) *Right to transfer title.* The Federal awarding agency may reserve the right to transfer title to the Federal Government or a third part named by the awarding agency when such a third party is otherwise eligible under existing statutes. Such transfers shall be subject to the following standards:

(1) The property shall be identified in the grant or otherwise made known to the grantee in writing.

(2) The Federal awarding agency shall issue disposition instruction within 120 calendar days after the end of the Federal support of the project for which it was acquired. If the Federal awarding agency fails to issue disposition instructions within the 120 calendar-day period the grantee shall follow §18.32(e).

(3) When title to equipment is transferred, the grantee shall be paid an amount calculated by applying the percentage of participation in the purchase to the current fair market value of the property.

8. [REQUIRED] Identify the format and timing of ISA reports to the Buyer/Parent Department. Include the type of reports (e.g., progress or status, data, etc.), timing of reports (e.g., weekly, monthly, final) and the medium for submission of reports (e.g., e-mail, Excel spreadsheet, paper, telephone):

Reporting Schedule

Quarter/Annual Report	Reporting Period	Due Date	Reporting Instrument/Format
1st Quarter	Oct 1 – Dec 31, 2017	January 10, 2018	EOPSS financial report/Excel and EOPSS progress report/Word
			BJA Online Performance Measurement Tool (PMT) Report
2nd Quarter	Jan 1 – Mar 31, 2018	April 10, 2018	EOPSS financial report/Excel and EOPSS progress report/Word
			BJA Online Performance Measurement Tool (PMT) Report
3rd Quarter	Apr 1 – Jun 30, 2018	July 10, 2018	EOPSS financial report/Excel and EOPSS progress report/Word
			BJA Online Performance Measurement Tool (PMT) Report
4th Quarter	Jul 1 – Sep 30, 2018	October 10, 2018	EOPSS financial report/Excel and EOPSS progress report/Word
			BJA Online Performance Measurement Tool (PMT) Report
5th Quarter-FINAL	Oct 1 – Dec 31, 2018	January 10, 2019	EOPSS financial report/Excel and EOPSS progress report/Word
			BJA Online Performance Measurement Tool (PMT) Report
Accounts Payable			EOPSS financial report/Excel and EOPSS progress report/Word
			BJA Online Performance Measurement Tool (PMT) Report

Reports Defined

All hard copies of quarterly financial and progress reports must be mailed and postmarked by the due date. Quarterly financial reports must include a copy of the CIW (warehouse) report for all cash and match expenditures.

9. Additional ISA Terms:

The following represent the Federal, Office of Grants and Research and Commonwealth general grant terms, as well as specific grant conditions. Note that some of the conditions do not pertain to the scope of services in this ISA, however, you must comply with all those conditions that are pertinent. **Note: Research related grant projects must respond to Section 6.**

Section : 1 Federal Grant Funds Sub-recipients

When receiving a grant award of federal funds administered by OGR, sub-recipients must comply with **three sets of *general* grant conditions**: (1) federal conditions; (2) state conditions; and (3) OGR conditions. These three sets of general conditions are discussed in this primary document.

Federal conditions are based on laws passed by Congress, regulations issued by the federal department making the funds available and published in the Code of Federal Regulations (CFR), and financial guidance documents also created by the federal department making

the funds available. Additionally in most cases, there are requirements and conditions associated with a *specific* federal grant stream which are not conditions of receipt of federal funds in general.

State conditions are established in laws passed by the Massachusetts Legislature and in orders and rules established by the Governor, and are referenced in the contract sub-recipients are required to execute. These conditions are found in the pages attached to the Standard Contract.

OGR conditions outline the further administrative requirements for each grant award established by EOPSS and OGR. They are included in this document.

Section 2: Basic Federal Grant Conditions

The basic federal grant conditions that follow apply to all federal grants, regardless of the federal department making the funds available.

- Audit Requirement of Federal Funds
  - OMB Circular A-133 requirements apply to each non-profit organization, each institution of higher education, and local governments as a whole when they or one of their departments receives federal funds. Any non-profit organization, institution of higher education, or local government spending more than $500,000 in federal funds *from all sources* within a 12-month period must have an audit performed on the use of the funds. OGR defines the 12-month period as July 1 to June 30. The following webpage provides the full text of this basic federal grant requirement: http://www.whitehouse.gov/sites/default/files/omb/assets/a133/a133_revised_2007.pdf

- Data Universal Number System (DUNS) and Central Contractor Registration (CCR)
  - All subrecipients of federal funds must have a nine-digit DUNS number in order. For more information: 1-866-705-5711 or http://fedgov.dnb.com/webform.
  - All subrecipients of federal funds must maintain annual registration in the CCR database: www.sam.gov

- Transparency Act Reporting for Federal Funds
  - The Federal Funding Accountability and Transparency Act (FFATA) requires EOPSS to report on a federal website specific award and subrecipient identifying information for each award greater than $25,000 OGR makes with federal funds it received after October 1, 2010. Prior to receiving funds, each affected subrecipient must report certain information to OGR so that EOPSS can fulfill its FFATA reporting requirements. Data reported by EOPSS may be viewed at www.USASpending.gov.

- Cost Principles for Federal Grants to *State and Local Governments*
  - 2 CFR Part 225 (formerly known as OMB Circular A-87) requirements apply only to state and local government subrecipients. These regulations list and define general categories of costs that are both allowable and unallowable. Examples are included below.
    - The cost of alcoholic beverages is unallowable.
    - Costs incurred by advisory councils are allowable.
    - Audit costs are allowable.
    - Compensation costs are allowable so long as they are consistent with that paid for similar work in other activities of the local government.
    - Entertainment costs are unallowable.
    - Equipment costs are allowable with the prior approval of OGR. Equipment having a useful life of more than one year or a current per-unit fair market value of $5,000 or more must be tracked. When replacing equipment purchased with federal funds, the equipment to be replaced may be used as a trade-in or can be sold with the proceeds used to offset the cost of the replacement equipment. In addition, during the period of the contract with OGR, insurance on the equipment is allowable. Information required to be captured and recorded appears in **Attachment A, Question 7.**
    - Travel costs are allowable if pre-approved by OGR and if they are consistent with costs normally allowed in like circumstances for non-federally funded activities. The following webpage provides the full text of this basic federal grant requirement: http://www.whitehouse.gov/omb/fedreg/2005/083105_a87.pdf.

    - If a subrecipient uses grant funds to pay its employees, the subrecipient must maintain timesheets for work performed with the grant funds. Timesheets must show the hours worked and must be signed by the employee paid with the grant funds.

- Cost Principles for Federal Grants to *Non-Profit Organizations and Institutions of Higher Education* requirements apply only to the non-profit and higher education subrecipients. The CFRs referenced below list and define general categories of costs that are allowable and unallowable. The links below provide the full text of these two basic federal grant requirements.
    - 2 CFR Part 220 pertains to Educational Institutions (formerly known as OMB Circular A-21): http://www.whitehouse.gov/omb/fedreg/2005/083105_a21.pdf.
    - 2 CFR Part 230 pertains to Non-profit Organizations (formerly known as OMB Circular A-122): http://www.whitehouse.gov/omb/fedreg/2005/083105_a122.pdf.

- Nondiscrimination Requirements
    - If you receive federal funds, you must comply with, and you must require your subcontractors, if any, to comply with, all applicable statutorily-imposed nondiscrimination requirements, which may include the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. § 3789d); the Victims of Crime Act (42 U.S.C. § 10604(e)); the Juvenile Justice and Delinquency Prevention Act of 2002 (42 U.S.C. § 5672(b)); the Civil Rights Act of 1964 (42 U.S.C. § 2000d); the Rehabilitation Act of 1973 (29 U.S.C. § 794); the Americans with Disabilities Act of 1990 (42 U.S.C. §§ 12131-34); the Education Amendments of 1972 (20 U.S.C. §§ 1681, 1683, 1685-86); the Age Discrimination Act of 1975 (42 U.S.C. §§ 6101-07); Ex. Order 13279 (equal protection of the laws for faith-based and community organizations); and 28 C.F.R. pt. 38 (U.S. Department of Justice Equal Treatment for Faith-Based Organizations).

    - Per Title VI of the Civil Rights Act of 1964 and the Omnibus Crime Control and Safe Streets Act of 1968, you must take reasonable steps to provide meaningful access for persons with limited English proficiency.

    - In the event a Federal or State court or Federal or State administrative agency makes a finding of discrimination after a due process hearing on the grounds of race, color, religion, national origin, sex, or disability against a recipient of funds, you must forward a copy of the finding to the Office for Civil Rights, Office of Justice Programs and to EOPSS/OGR.

    - In accordance with federal civil rights laws, you shall not retaliate against individuals for taking action or participating in action to secure rights protected by these laws.

- Human Subjects Protection (for research subrecipients only, see Addendum 1).

Section 3: Additional Federal Department-Dependent Grant Conditions

In addition to the basic federal grant conditions, each federal department that is the source of the funds may impose additional conditions. If you are awarded funds by OGR that originate from any of the federal departments listed below, you should be familiar with the text from each of the applicable links.

U.S. Department of Justice Funds

The U.S. Department of Justice offers a Financial Guide that presents grant requirements as defined by this federal agency. All subrecipients of these funds must adhere to these requirements.

- The webpage for the US DOJ Financial Guide is as follows: http://www.ojp.usdoj.gov/financialguide/index.htm.

    Pay particular attention to the sections on (1) matching or cost sharing, (2) allowable costs, (3) unallowable costs, (4) procurement under awards of federal assistance, (5) costs requiring prior approval, (6) equipment, and (7) retention and access requirements for records.

- If you receive DOJ grant funds, you may be required to comply with the regulatory requirement to develop, maintain on file, and submit for review to the Office for Civil Rights, Office of Justice Programs and to OGR an Equal Employment Opportunity Plan (EEOP). The url for DOJ's system for implementing this requirement is as follows: http://www.ojp.usdoj.gov/about/ocr/eeop_comply.htm

Section 4: Office of Grants and Research Conditions

In addition to the federal and state general grant conditions outlined above, the Office of Grants and Research (OGR) in the Executive Office of Public Safety and Security (EOPSS) has certain grant conditions that are essential to the administration of grant awards. Whether subrecipients are receiving funds from a federal or state grant, they must adhere to these conditions.

- **Federal *and* State Conditions** must be adhered to by subrecipients of federal grant funds.

- **Time extensions** of contracts, while uncommon, may be granted at the option of OGR. They are not encouraged or guaranteed.
    - If a subrecipient needs additional time to complete the scope of work for the grant award, OGR may grant a time-only extension as long as the revised contract containing the extension request is executed by both the subrecipient and OGR before the current end date of the contract. No time extension can be granted if the revised contract form is executed after the current end date of the contract.
    - Requests for time extensions must to be made at least 30 days before the end date of the contract.
- **Award amounts remaining at the end of the ISA/contract** will be reverted back to OGR. All goods must be received and all services rendered by the end date of the contract.
- **Each ISA has a defined accounts payable period. All payments must be made for services rendered or goods received by the end of this period.**
- **An ISA that crosses a state fiscal year (June 30) into the next fiscal year must observe the Commonwealth's policies on payment corrections or overpayments. That is, any mistakes in coding must be corrected with an EX transaction before August 31. All payroll corrections must be made by the date in July specified in the Fiscal Year Open/Close guidance issued each year by the Office of the State Comptroller. Any overpayments must be made corrected with an ER transaction before August 31.**
- **EPS certifies that the start date is the date the funds are loaded into MMARS and available to the child department.**
- **Programmatic and financial reports** must be received in accordance with the requirements of the specific award. At the option of OGR, reimbursement will be held until all reporting requirements are met.
- **Allowable grant-related travel costs** charged to grant awards will currently be paid at the lesser of $.45 per mile or the subrecipient's normal reimbursement rate. This rate is subject to change. Tolls and parking for grant-related local travel may also be paid. Receipts are required.
- **Indirect cost rates** will not be reimbursed based on a percentage rate without documentation of the rate having been approved by a federal agency. When a percentage rate has not been approved by a federal agency, a subrecipient may request of OGR allowable direct costs that will be incurred and can be specifically allocated to the project being funded.
- **Procurement practices** of subrecipient agencies must be followed. The subrecipient should ensure that its procurement practices conform to any specific federal guidelines found in the references in the federal conditions section above. Where there is a difference between the practices of the subrecipient agency/organization and a federal guideline, the more restrictive procedure applies.
- **Timesheets** must be maintained by subrecipients for work performed by its employee(s) paid for with grant funds. Timesheets must show the hours worked and paid for with grant funds and must be signed by the employee(s).
- **Submission of "Federal OMB Circular A-133 Audit Form**" is required for subrecipients that receive more than $500,000 in federal funds from all sources. OGR has developed a "self-identifying" form titled "Federal OMB Circular A-133 Audit Form" to be submitted to OGR at the end of the fiscal year and after the completion of an A-133 federal funds audit. The form asks if the subrecipient was required to have an audit and, if so, to identify any findings related to the federal funds awarded by OGR.
- **Site visits** to subrecipients will be made by OGR periodically. All records, papers, and other documents of any kind related to the funded activity must be made promptly available upon request for inspection and copying to any person authorized by OGR.
- **Grant-related documents** must be retained for a period of six years from the close of the contract.
- **Evaluations** of a subrecipient's funded program by an outside evaluator during or at the conclusion of the project period, should be reported to OGR in writing and a copy of the evaluation should be provided.
- **Reporting alleged fraud, waste or abuse** to the Office of the State Auditor or Inspector General and/or to an applicable federal agency is the responsibility of the subrecipient. This includes any alleged violations, serious irregularities, sensitive issues or overt or covert acts involving the use of public funds in a manner not consistent with federal statutes, related laws and regulations, appropriate guidelines, or purposes of the grant.
- **Use of funds should begin** within 60 days of the start of the contract, and if they are not, the subrecipient must report to OGR the steps taken to initiate the grant activities, the reasons for the delay, and the expected start of the use of the funds. If meaningful implementation steps have not begun after 60 days of the grant start date, OGR reserves the right to cancel the contract.
- **Subcontractors** implementing activities with grant funds must adhere to the grant provisions in this document and should be approved by OGR prior to subrecipients executing subcontracts.
- **Instructional materials** created or produced with grant funds will be "work made for hire," as defined in United States copyright law, and EOPSS shall be considered the author. EOPSS shall be the sole owner of all rights pertaining to these materials, including copyrights and all rights to use, reproduce, or publish the materials, and subrecipients may not use, reproduce, or distribute such materials without prior written approval of OGR. If a project results in the production of **other original books, manuals, or copyrightable material**, unless otherwise provided in the contract documents, EOPSS reserves

a royalty-free, non-exclusive and irrevocable license to reproduce, publish, translate or otherwise use, and authorize others to publish and use, such material. If paid with federal funds, the grant number must appear on the materials.

- **Audio visual or written materials** developed as part of the grant may be required to incorporate specific language or disclaimers (e.g., regarding the federal source of funding) and in some instances pre-approval from the federal funding agency as instructed by the OGR grants manager.

Section 5: Additional OGR Conditions for Law Enforcement Agencies

Law enforcement agencies are subject to mandatory reporting requirements of various information, including, but not limited to the reporting requirements listed below. EOPSS and OGR may withhold reimbursements, cancel your contract, or withhold execution of any future grants for law enforcement agencies that do not comply with reporting requirements.

- ***Crime Data Reporting.*** Law enforcement organizations must submit timely and satisfactory monthly Uniform Crime Reporting (UCR) or National Incident Based Reporting System (NIBRS) reports to the Commonwealth's Crime Reporting Unit at the Commonwealth Fusion Center. If your organization has hardware and software that support the creation of NIBRS data, crime data must be submitted to the Crime Reporting Unit in that format.

- ***Motor Vehicle Accident Reporting.*** Police departments are required to report to the Registry of Motor Vehicles, within 15 days, accidents in which death, injury, or property damage in excess of $1,000 occurs (M.G.L. c. 90, § 29). The crash reports can be delivered to the Registry of Motor Vehicles (RMV) main office through post office mail or through electronic submission. You may contact the RMV headquarters for any additional information.

- ***Juvenile Lockup Data.*** Law enforcement agencies that maintain a juvenile lockup must submit monthly juvenile lockup data to the Department of Criminal Justice Information Services via CJIS/LEAPS. Contact OGR's Juvenile Justice Program Coordinator for additional information.

- ***Fingerprint Cards.*** Law enforcement agencies must regularly submit fingerprint cards for all felony arrests to the Identification Section at the Massachusetts State Police Crime Lab as required by state law (M.G.L. c. 263, § 1A; G.L. c. 94C, § 45).

Section 6: Additional OGR Conditions for Research Grants Only: Human Subjects Protection

Research subrecipients must check one of the statements below.

[ ] a. The research activities covered under this Contract/ISA do not involve human subjects.
[ ] b. The research activities covered under this Contract/ISA do involve human subjects.

If the research activities involve human subjects (option b), then the subrecipient agrees to certify compliance with 28 C.F.R. Part 46 regulations by completing, "Protection of Human Subjects, IRB Certification, Declaration of Exemption (Common Rule)." This form is available at the National Institute of Justice webpage at http://www.ojp.usdoj.gov/nij/funding/humansubjects/human-subjects.htm

The regulation for The Protection of Human Subjects 28 C.F.R Part 46 section 46.101(b)(1-6) defines categories of research involving human subjects that are exempt from its provisions. Details on exemptions can be found at the same National Institute of Justice webpage listed above.

***SPECIFIC CONDITIONS for JAG Award* # 2016-DJBX-0653**

1. Applicability of Part 200 Uniform Requirements

The Uniform Administrative Requirements, Cost Principles, and Audit Requirements in 2 C.F.R. Part 200, as adopted and supplemented by the Department of Justice (DOJ) in 2 C.F.R. Part 2800 (the "Part 200 Uniform Requirements") apply to this 2016 award from the Office of Justice Programs (OJP). For this 2015 award, the Part 200 Uniform Requirements, which were first adopted by DOJ on December 26, 2014, supersede, among other things, the provisions of 28 C.F.R. Parts 66 and 70, as well as those of 2 C.F.R. Parts 215, 220, 225, and 230.

If this 2016 award supplements funds previously awarded by OJP under the same award number, the Part 200 Uniform Requirements apply with respect to all award funds (whether derived from the initial award or a supplemental award) that are obligated on or after the acceptance date of this 2015 award.

Potential availability of grace period for procurement standards: Under the Part 200 Uniform Requirements, a time limited grace period may be available under certain circumstances to allow for transition from policies and procedures that complied with previous standards for procurements under federal awards to policies and procedures that comply with the new standards (that is, to those at 2 C.F.R. 200.317 through 200.326).

For more information on the Part 200 Uniform Requirements, including information regarding the potentially-available grace period described above, see the Office of Justice Programs (OJP) website at http://ojp.gov/funding/Part200UniformRequirements.htm.

In the event that an award-related question arises from documents or other materials prepared or distributed by OJP that may appear to conflict with, or differ in some way from, the provisions of the Part 200 Uniform Requirements, the recipient is to contact OJP promptly for clarification.

2. The recipient agrees to comply with the Department of Justice Grants Financial Guide as posted on the OJP website (currently, the "2016 DOJ Grants Financial Guide").

3. The recipient acknowledges that failure to submit an acceptable Equal Employment Opportunity Plan (if recipient is required to submit one pursuant to 28 C.F.R. Section 42.302) that is approved by the Office for Civil Rights is a violation of the Standard Assurances executed by the recipient, and may result in suspension of funding until such time as the recipient is in compliance, or termination of the award.

4. The recipient understands and agrees that OJP may withhold award funds, or may impose other related requirements, if the recipient does not satisfactorily and promptly address outstanding issues from audits required by the Part 200 Uniform Requirements (or by the terms of this award), or other outstanding issues that arise in connection with audits, investigations, or reviews of DOJ awards.

5. Recipient understands and agrees that it cannot use any federal funds, either directly or indirectly, in support of the enactment, repeal, modification or adoption of any law, regulation or policy, at any level of government, without the express prior written approval of OJP.

6. The recipient and any sub recipients must promptly refer to the DOJ OIG any credible evidence that a principal, employee, agent, sub recipient, contractor, subcontractor, or other person has -- (1) submitted a claim for award funds that violates the False Claims Act; or (2) committed a criminal or civil violation of laws pertaining to fraud, conflict of interest, bribery, gratuity, or similar misconduct involving award funds. Potential fraud, waste, abuse, or misconduct should be reported to the OIG by - mail: Office of the Inspector General U.S. Department of Justice Investigations Division 950 Pennsylvania Avenue, N.W. Room 4706 Washington, DC 20530 e-mail: oig.hotline@usdoj.gov hotline: (contact information in English and Spanish): (800) 869-4499 or hotline fax: (202) 616-9881 Additional information is available from the DOJ OIG website at www.usdoj.gov/oig

7. Restrictions and certifications regarding non-disclosure agreements and related matters

No recipient or subrecipient under this award, or entity that receives a contract or subcontract with any funds under this award, may require any employee or contractor to sign an internal confidentiality agreement or statement that prohibits or otherwise restricts, or purports to prohibit or restrict, the reporting (in accordance with law) of waste, fraud, or abuse to an investigative or law enforcement representative of a federal department or agency authorized to receive such information.

The foregoing is not intended, and shall not be understood by the agency making this award, to contravene requirements applicable to Standard Form 312 (which relates to classified information), Form 4414 (which relates to sensitive compartmented information), or any other form issued by a federal department or agency governing the nondisclosure of classified information.

1. In accepting this award, the recipient --

a. represents that it neither requires nor has required internal confidentiality agreements or statements from employees or contractors that currently prohibit or otherwise currently restrict (or purport to prohibit or restrict) employees or contractors from reporting waste, fraud, or abuse as described above; and

b. certifies that, if it learns or is notified that it is or has been requiring its employees or contractors to execute agreements or statements that prohibit or otherwise restrict (or purport to prohibit or restrict), reporting of waste, fraud, or abuse as described above, it will immediately stop any further obligations of award funds, will provide prompt written notification to the agency making this award, and will resume (or permit resumption of)such obligations only if expressly authorized to do so by that agency.

2. If the recipient does or is authorized to make subawards or contracts under this award --

a. it represents that --

(1) it has determined that no other entity that the recipient's application proposes may or will receive award funds (whether through a subaward, contract, or subcontract) either requires or has required internal confidentiality agreements or statements from employees or contractors that currently prohibit or otherwise currently restrict (or purport to prohibit or restrict) employees or contractors from reporting waste, fraud, or abuse as described above; and

(2) it has made appropriate inquiry, or otherwise has an adequate factual basis, to support this representation; and

b. it certifies that, if it learns or is notified that any subrecipient, contractor, or subcontractor entity that receives funds under this award is or has been requiring its employees or contractors to execute agreements or statements that prohibit or otherwise restrict (or purport to prohibit or restrict), reporting of waste, fraud, or abuse as described above, it will immediately stop any further obligations of award funds to or by that entity, will provide prompt written notification to the agency making this award, and will resume (or permit resumption of) such obligations only if expressly authorized to do so by that agency.

8. Recipient understands and agrees that it cannot use any federal funds, either directly or indirectly, in support of any contract or subaward to either the Association of Community Organizations for Reform Now (ACORN) or its subsidiaries, without the express prior written approval of OJP.

9. The recipient agrees to comply with any additional requirements that may be imposed during the grant performance period if the agency determines that the recipient is a high-risk grantee. Cf. 28 C.F.R. parts 66, 70.

10. The recipient agrees to comply with applicable requirements regarding registration with the System for Award Management (SAM) (or with a successor government-wide system officially designated by OMB and OJP). The recipient also agrees to comply with applicable restrictions on subawards to first-tier subrecipients that do not acquire and provide a Data Universal Numbering System (DUNS) number. The details of recipient obligations are posted on the Office of Justice Programs web site at http://www.ojp.gov/funding/sam.htm (Award condition: Registration with the System for Award Management and Universal Identifier Requirements), and are incorporated by reference here. This special condition does not apply to an award to an individual who received the award as a natural person (i.e., unrelated to any business or non-profit organization that he or she may own or operate in his or her name).

11. Pursuant to Executive Order 13513, "Federal Leadership on Reducing Text Messaging While Driving," 74 Fed. Reg. 51225 (October 1, 2009), the Department encourages recipients and sub recipients to adopt and enforce policies banning employees from text messaging while driving any vehicle during the course of performing work funded by this grant, and to establish workplace safety policies and conduct education, awareness, and other outreach to decrease crashes caused by distracted drivers.

12. The recipient agrees to comply with all applicable laws, regulations, policies, and guidance (including specific cost limits, prior approval and reporting requirements, where applicable) governing the use of federal funds for expenses related to conferences, meetings, trainings, and other events, including the provision of food and/or beverages at such events, and costs of attendance at such events. Information on rules applicable to this award appears in the DOJ Grants Financial Guide (currently, as section 3.10 of "Postaward Requirements" in the "2015 DOJ Grants Financial Guide").

13. The recipient understands and agrees that any training or training materials developed or delivered with funding provided under this award must adhere to the OJP Training Guiding Principles for Grantees and Subgrantees, available at http://www.ojp.usdoj.gov/funding/ojptrainingguidingprinciples.htm.

14.The recipient agrees that if it currently has an open award of federal funds or if it receives an award of federal funds other than this OJP award, and those award funds have been, are being, or are to be used, in whole or in part, for one or more of the identical cost items for which funds are being provided under this OJP award, the recipient will promptly notify, in writing, the grant manager for this OJP award, and, if so requested by OJP, seek a budget modification or change-of-project-scope grant adjustment notice (GAN) to eliminate any inappropriate duplication of funding.

15. The recipient understands and agrees that award funds may not be used to discriminate against or denigrate the religious or moral beliefs of students who participate in programs for which financial assistance is provided from those funds, or of the parents or legal guardians of such students.

16. The recipient understands and agrees that - (a) No award funds may be used to maintain or establish a computer network unless such network blocks the viewing, downloading, and exchanging of pornography, and (b) Nothing in subsection (a) limits the use of funds necessary for any Federal, State, tribal, or local law enforcement agency or any other entity carrying out criminal investigations, prosecution, or adjudication activities.

17. A recipient that is eligible under the Part 200 Uniform Requirements to use the "de minimis" indirect cost rate described in 2 C.F.R. 200.414(f), and that elects to use the "de minimis" indirect cost rate, must advise OJP in writing of both its eligibility and its election, and must comply with all associated requirements in the Part 200 Uniform Requirements. The "de minimis" rate may be applied only to modified total direct costs (MTDC).

18. The recipient must collect, maintain, and provide to OJP, data that measure the performance and effectiveness of activities under this award, in the manner, and within the timeframes, specified in the program solicitation, or as otherwise specified by OJP. Data collection supports compliance with the Government Performance and Results Act (GPRA) and the GPRA Modernization Act, and other applicable laws.

19. The recipient agrees to comply with OJP grant monitoring guidelines, protocols, and procedures, and to cooperate with BJA and OCFO on all grant monitoring requests, including requests related to desk reviews, enhanced programmatic desk reviews, and/or site visits. The recipient agrees to provide to BJA and OCFO all documentation necessary to complete monitoring tasks, including documentation related to any subawards made under this award. Further, the recipient agrees to abide by reasonable deadlines set by BJA and OCFO for providing the requested documents. Failure to cooperate with BJA's/OCFO's grant monitoring activities may result in sanctions affecting the recipient's DOJ awards, including, but not limited to: withholdings and/or other restrictions on the recipient's access to grant funds; referral to the Office of the Inspector General for audit review; designation of the recipient as a DOJ High Risk grantee; or termination of an award(s).

20. The recipient agrees to comply with applicable requirements to report first-tier subawards of $25,000 or more and, in certain circumstances, to report the names and total compensation of the five most highly compensated executives of the recipient and first-tier subrecipients of award funds. Such data will be submitted to the FFATA Subaward Reporting System (FSRS). The details of recipient obligations, which derive from the Federal Funding Accountability and Transparency Act of 2006 (FFATA), are posted on the Office of Justice Programs web site at http://www.ojp.gov/funding/ffata.htm (Award condition: Reporting Subawards and Executive Compensation), and are incorporated by reference here. This condition, and its reporting requirement, does not apply to grant awards made to an individual who received the award as a natural person (i.e., unrelated to any business or non-profit organization that he or she may own or operate in his or her name).

21. The recipient understands and agrees that it has a responsibility to monitor its subrecipients' compliance with applicable federal civil rights laws. The recipient agrees to submit written Methods of Administration (MOA) for ensuring subrecipients' compliance to the OJP's Office for Civil Rights at CivilRightsMOA@usdoj.gov within 90 days of receiving the grant award, and to make supporting documentation available for review upon request by OJP or any other authorized persons. The required elements of the MOA are set forth at http://www.ojp.usdoj.gov/funding/other_requirements.htm, under the heading, "Civil Rights Compliance Specific to State Administering Agencies."

22. In order to promote information sharing and enable interoperability among disparate systems across the justice and public safety community, OJP requires the grantee to comply with DOJ's Global Justice Information Sharing Initiative (DOJ's Global) guidelines and recommendations for this particular grant. Grantee shall conform to the Global Standards Package (GSP) and all constituent elements, where applicable, as described at: http://www.it.ojp.gov/gsp_grantcondition. Grantee shall document planned approaches to information sharing and describe compliance to the GSP and appropriate privacy policy that protects shared information, or provide detailed justification for why an alternative approach is recommended.

23. To avoid duplicating existing networks or IT systems in any initiatives funded by BJA for law enforcement information sharing systems which involve interstate connectivity between jurisdictions, such systems shall employ, to the extent possible, existing

networks as the communication backbone to achieve interstate connectivity, unless the grantee can demonstrate to the satisfaction of BJA that this requirement would not be cost effective or would impair the functionality of an existing or proposed IT system.

24. Approval of this award does not indicate approval of any consultant rate in excess of $650 per day. A detailed justification must be submitted to and approved by the Office of Justice Programs (OJP) program office prior to obligation or expenditure of such funds.

25. All procurement (contract) transactions under this award must be conducted in a manner that is consistent with applicable Federal and State law, and with Federal procurement standards specified in regulations governing Federal awards to non-Federal entities. Procurement (contract) transactions should be competitively awarded unless circumstances preclude competition. Noncompetitive (e.g., sole source) procurements by the award recipient in excess of the Simplified Acquisition Threshold (currently $150,000) set out in the Federal Acquisition Regulation must receive prior approval from the awarding agency, and must otherwise comply with rules governing such procurements found in the current edition of the OJP Financial Guide.

26. The recipient agrees to participate in BJA-sponsored training events, technical assistance events, or conferences held by BJA or its designees, upon BJA's request.

27. The grantee agrees that within 120 days of award acceptance, each current member of a law enforcement task force funded with these funds who is a task force commander, agency executive, task force officer, or other task force member of equivalent rank, will complete required online (internet-based) task force training. Additionally, all future task force members are required to complete this training once during the life of this award, or once every four years if multiple awards include this requirement. The training is provided free of charge online through BJA's Center for Task Force Integrity and Leadership (www.ctfli.org). This training addresses task force effectiveness as well as other key issues including privacy and civil liberties/rights, task force performance measurement, personnel selection, and task force oversight and accountability. When BJA funding supports a task force, a task force personnel roster should be compiled and maintained, along with course completion certificates, by the grant recipient. Additional information is available regarding this required training and access methods via BJA's web site and the Center for Task Force Integrity and Leadership (www.ctfli.org).

28. Award recipients must verify Point of Contact (POC), Financial Point of Contact (FPOC), and Authorized Representative contact information in GMS, including telephone number and e-mail address. If any information is incorrect or has changed, a Grant Adjustment Notice (GAN) must be submitted via the Grants Management System
(GMS) to document changes.

29. Grantee agrees to comply with all confidentiality requirements of 42 U.S.C. section 3789g and 28 C.F.R. Part 22 that are applicable to collection, use, and revelation of data or information. Grantee further agrees, as a condition of grant approval, to submit a Privacy Certificate that is in accord with requirements of 28 C.F.R. Part 22 and, in particular, section 22.23.

30. Grantee agrees to comply with the requirements of 28 C.F.R. Part 46 and all Office of Justice Programs policies and procedures regarding the protection of human research subjects, including obtainment of Institutional Review Board approval, if appropriate, and subject informed consent.

31. The grantee agrees to comply with the applicable requirements of 28 C.F.R. Part 38, the Department of Justice regulation governing "Equal Treatment for Faith Based Organizations" (the "Equal Treatment Regulation"). The Equal Treatment Regulation provides in part that Department of Justice grant awards of direct funding may not be used to fund any inherently religious activities, such as worship, religious instruction, or proselytization. Recipients of direct grants may still engage in inherently religious activities, but such activities must be separate in time or place from the Department of Justice funded program, and participation in such activities by individuals receiving services from the grantee or a sub-grantee must be voluntary. The Equal Treatment Regulation also makes clear that organizations participating in programs directly funded by the Department of Justice are not permitted to discriminate in the provision of services on the basis of a beneficiary's religion. Notwithstanding any other special condition of this award, faithbased organizations may, in some circumstances, consider religion as a basis for employment. See http://www.ojp.gov/about/ocr/equal_fbo.htm.

32. The recipient agrees that any information technology system funded or supported by OJP funds will comply with 28 C.F.R. Part 23, Criminal Intelligence Systems Operating Policies, if OJP determines this regulation to be applicable. Should OJP determine 28 C.F.R. Part 23 to be applicable, OJP may, at its discretion, perform audits of the system, as per the regulation. Should any violation of 28 C.F.R. Part 23 occur, the recipient may be fined as per 42 U.S.C. 3789g(c)-(d). Recipient may not satisfy such a fine with federal funds.

33. Program income (as defined in the Part 200 Uniform Requirements) must be used in accordance with the provisions of the Part 200 Uniform Requirements. Program income earnings and expenditures both must be reported on the quarterly Federal Financial Report, SF 425.

34. Award recipients must submit quarterly a Federal Financial Report (SF-425) and annual performance reports through GMS (https://grants.ojp.usdoj.gov). Consistent with the Department's responsibilities under the Government Performance and Results Act (GPRA), P.L. 103-62, applicants who receive funding under this solicitation must provide data that measure the results of their work. Therefore, quarterly performance metrics reports must be submitted through BJA's Performance Measurement Tool (PMT) website (www.bjaperformancetools.org). For more detailed information on reporting and other JAG requirements, refer to the JAG reporting requirements webpage. Failure to submit required JAG reports by established deadlines may result in the freezing of grant funds and future High Risk designation.

35. The recipient agrees that funds received under this award will not be used to supplant State or local funds, but will be used to increase the amounts of such funds that would, in the absence of Federal funds, be made available for law enforcement activities.

36. The recipient agrees to monitor subawards under this JAG award in accordance with all applicable statutes, regulations, OMB circulars, and guidelines, including the OJP Financial Guide, and to include the applicable conditions of this award in any subaward. The recipient is responsible for oversight of subrecipient spending and monitoring of specific outcomes and benefits attributable to use of JAG funds by subrecipients. The recipient agrees to submit, upon request, documentation of its policies and procedures for monitoring of subawards under this award.

37. The recipient agrees to submit a signed certification that that all law enforcement agencies receiving vests purchased with JAG funds have a written "mandatory wear" policy in effect. Fiscal agents and state agencies must keep signed certifications on file for any subrecipients planning to utilize JAG funds for ballistic-resistant and stab-resistant body armor purchases. This policy must be in place for at least all uniformed officers before any JAG funding can be used by the agency for body armor. There are no requirements regarding the nature of the policy other than it being a mandatory wear policy for all uniformed officers while on duty.

38. Ballistic-resistant and stab-resistant body armor purchased with JAG funds may be purchased at any threat level, make or model, from any distributor or manufacturer, as long as the vests have been tested and found to comply with applicable National Institute of Justice ballistic or stab standards and are listed on the NIJ Compliant Body Armor Model List (http://nij.gov). In addition, ballistic-resistant and stab-resistant body armor purchased must be American made. The latest NIJ standard information can be found here: http://www.nij.gov/topics/technology/body-armor/safetyinitiative. htm.

39. JAG funds may be used to purchase vests for an agency, but they may not be used as the 50% match for purposes of the Bulletproof Vest Partnership (BVP) program.

40. The recipient is required to establish a trust fund account. (The trust fund may or may not be an interest-bearing account.) The fund, including any interest, may not be used to pay debts or expenses incurred by other activities beyond the scope of the Edward Byrne Memorial Justice Assistance Grant Program (JAG). The recipient also agrees to obligate the grant funds in the trust fund (including any interest earned) during the period of the grant and expend within 90 days thereafter. Any unobligated or unexpended funds, including interest earned, must be returned to the Office ofJustice Programs at the time of closeout.

41. The grantee agrees to assist BJA in complying with the National Environmental Policy Act (NEPA), the National Historic Preservation Act, and other related federal environmental impact analyses requirements in the use of these grant funds, either directly by the grantee or by a subgrantee. Accordingly, the grantee agrees to first determine if any of the following activities will be funded by the grant, prior to obligating funds for any of these purposes. If it is determined that any of the following activities will be funded by the grant, the grantee agrees to contact BJA.

The grantee understands that this special condition applies to its following new activities whether or not they are being specifically funded with these grant funds. That is, as long as the activity is being conducted by the grantee, a subgrantee, or any third party and the activity needs to be undertaken in order to use these grant funds, this special condition must first be met. The activities covered by this special condition are:
a. New construction;
b. Minor renovation or remodeling of a property located in an environmentally or historically sensitive area, including properties located within a 100-year flood plain, a wetland, or habitat for endangered species, or a property listed on or eligible for listing on the National Register of Historic Places;
c. A renovation, lease, or any proposed use of a building or facility that will either (a) result in a change in its basic prior use or (b) significantly change its size;

d. Implementation of a new program involving the use of chemicals other than chemicals that are (a) purchased as an incidental component of a funded activity and (b) traditionally used, for example, in office, household, recreational, or education environments; and

e. Implementation of a program relating to clandestine methamphetamine laboratory operations, including the identification, seizure, or closure of clandestine methamphetamine laboratories.

The grantee understands and agrees that complying with NEPA may require the preparation of an Environmental Assessment and/or an Environmental Impact Statement, as directed by BJA. The grantee further understands and agrees to the requirements for implementation of a Mitigation Plan, as detailed at http://www.ojp.usdoj.gov/BJA/resource/nepa.html, for programs relating to methamphetamine laboratory operations.

Application of This Special Condition to Grantee's Existing Programs or Activities: For any of the grantee's or its subgrantees' existing programs or activities that will be funded by these grant funds, the grantee, upon specific request from BJA, agrees to cooperate with BJA in any preparation by BJA of a national or program environmental assessment of that funded program or activity.

42. BJA strongly encourages the recipient to submit annual (or more frequent) JAG success stories. To submit a success story, sign in to your My BJA account at https://www.bja.gov/Login.aspx to access the Success Story Submission form. If you do not yet have a My BJA account, please register at https://www.bja.gov/profile.aspx. Once you register, one of the available areas on your My BJA page will be "My Success Stories". Within this box, you will see an option to add a Success Story. Once reviewed and approved by BJA, all success stories will appear on the new BJA Success Story web page at https://www.bja.gov/SuccessStoryList.aspx.

43. Recipient understands and agrees that award funds may not be used for items that are listed on the Prohibited Expenditure List at the time of purchase or acquisition, including as the list may be amended from time to time. The Prohibited Expenditure list may be accessed here: https://www.bja.gov/funding/JAGControlledPurchaseList.pdf.

44. Recipient understands and agrees that award funds may not be used for items that are listed on the Controlled Expenditure List at the time of purchase or acquisition, including as the list may be amended from time to time, without explicit written prior approval from BJA. The Controlled Expenditure List and instructions on how to request approval for purchase or acquisitions may be accessed here: https://www.bja.gov/funding/JAGControlledPurchaseList.pdf

45. Recipient understands and agrees that the purchase or acquisition of any item on the Controlled Expenditure List at the time of purchase or acquisition, including as the list may be amended from time to time, with award funds by an agency will trigger a requirement that the agency collect and retain (for at least 3 years) certain information about the use of 1) any federally-acquired Controlled Equipment in the agency's inventory, and 2) any other controlled equipment in the same category as the federally-acquired controlled equipment in the agency's inventory, regardless of source; and make that information available to BJA upon request. Details about what information must be collected and retained may be accessed here: https://www.whitehouse.gov/sites/default/files/docs/le_equipment_wg_final_report_final.pdf

46. Recipient understands and agrees that, notwithstanding 2 CFR § 200.313, no equipment listed on the Controlled Expenditure List that is purchased under this award may be transferred or sold to a third party, except as described below:

a. Agencies may transfer or sell any controlled equipment, except riot helmets and riot shields, to a Law Enforcement Agency (LEA) after obtaining prior written approval from BJA. As a condition of that approval, the acquiring LEA will be required to submit information and certifications to BJA as if it was requesting approval to use award fund for the initial purchase of items on the Controlled Expenditure List.

b. Agencies may not transfer or sell any riot helmets or riot shields purchased under this award.

c. Agencies may not transfer or sell any Controlled Equipment purchased under this award to non-LEAs, with the exception of fixed wing aircraft, rotary wing aircraft, and command and control vehicles. Before any such transfer or sale is finalized, the agency must obtain prior written approval from BJA. All law enforcement-related and other sensitive or potentially dangerous components, and all law enforcement insignias and identifying markings must be removed prior to transfer or sale.

Recipient further understands and agrees to notify BJA prior to the disposal of any items on the Controlled Expenditure List purchased under this award, and to abide by any applicable laws and regulations in such disposal.

47. Recipient understands and agrees that failure to comply with conditions related to Prohibited or Controlled

Expenditures may result in a prohibition from further Controlled Expenditure approval under this or other federal awards.

48. Recipient acknowledges the final agency decision made by the U.S. Department of Justice that recipient's jurisdiction did not substantially implement the Sex Offender Registration and Notification Act (P.L. 109-248) before the deadline, which determination impacts the funding amount of this award, pursuant to 42 U.S.C. § 16925. In accepting this specific formula award, recipient hereby voluntarily agrees that if it elects to file a judicial appeal of that final agency decision, which was integral in determining this particular funding amount, no such appeal may commence more than 6 months after the date of this award.

49. With respect to this award, federal funds may not be used to pay cash compensation (salary plus bonuses) to any employee of the award recipient at a rate that exceeds 110% of the maximum annual salary payable to a member of the federal government's Senior Executive Service (SES) at an agency with a Certified SES Performance Appraisal System for that year. (An award recipient may compensate an employee at a higher rate, provided the amount in excess of this compensation limitation is paid with non-federal funds.)

This limitation on compensation rates allowable under this award may be waived on an individual basis at the discretion of the OJP official indicated in the program announcement under which this award is made.

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM
ATTACHMENT B - BUDGET

Check one: _X_ Initial ISA Budget

____ ISA Budget/Account Amendment. Maximum Obligation of ISA before this Amendment: $_____.

PRIOR MMARS DOCUMENT ID: _____ (for reference - if applicable)

CURRENT DOC ID: ISAEPSJG16HEROPOL18A.

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

A Budget Fiscal Year	B Seller/Child Account	C Object Class	D Description	E Initial ISA Amount / or Amount Prior to Amendment	F Indicate Add or Reduce +/-	G Amendment Amount	H Enter "YES" if Amount is a prior FY budget reduction or a current FY "Carry-in" authorization for Federal ISA Funds	I New Amount After Amendment
				$		$		$
				$		$		$
				$		$		$
				$		$		$
				$		$		$
				$		$		$
				$		$		$
				$		$		$
				$		$		$
				$		$		$
				$		$		$
				$		$		$

FISCAL YEAR SUBTOTALS AND TOTAL MAXIMUM OBLIGATION FOR DURATION OF ISA	
FISCAL YEAR: _2017_____ SUBTOTAL (*or New Subtotal if Fiscal Year Subtotal being amended*	$
FISCAL YEAR: __2018_____ SUBTOTAL (*or New Subtotal if Fiscal Year Subtotal being amended*	$
FISCAL YEAR: _____ SUBTOTAL (*or New Subtotal if Fiscal Year Subtotal being amended*	$
FISCAL YEAR: _____ SUBTOTAL (*or New Subtotal if Fiscal Year Subtotal being amended*	$
TOTAL MAXIMUM OBGLIGATON FOR DURATION OF ISA (*or New Total Maximum Obligation if amended*)	$97,946.80

Additional Budget Specifications:

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM
ATTACHMENT C – FEDERAL GRANT SELLER/CHILD ACCOUNT

[Complete ONLY if Buyer/Parent Account is a Federal Grant Account. Seller/Child Department must signoff in order to process document.]

__X__ NEW ISA ___ ISA AMENDMENT	**BUDGET FISCAL YEAR: 2018**
BUYER/PARENT DEPARTMENT: EPS	**SELLER/CHILD DEPARTMENT: POL**
CTR ONLY - REVENUE BUREAU WILL ASSIGN	
Revenue Budget	Revenue Source
BUYER/PARENT DEPARTMENT MUST COMPLETE ALL ITEMS BELOW	
CENTRAL BUDGET STRUCTURE (BGCN - BQ89)	
Appropriation Number: 80004611	Payroll Indicator : __X__ Yes ___ No
Budgetary Estimated Receipts $	BGCN Document Identification No.: ISAEPSJG16HEROPOL18A
COST ACCOUNTING STRUCTURE (BGRG- BQ88)	
Total Maximum Obligation of ISA: $97,946.80	BGRG Document Identification No.: ISAEPSJG16HEROPOL18A
MAJOR PROGRAM TABLE SET-UP	
Major Program (6 chars. or less): BJAG	Major Program Short Name (same as appropriation number): 80004611
Major Program Name: Byrne Justice Assistance Grant	
PROGRAM PERIOD TABLE SET-UP OR EXTENDED PROGRAM PERIOD	
Effective From Date: 05/22/2009	Effective To Date: 06/30/2020
Program Period: EPP	
Program Period Name: EPP	Program Period Short Name: EPP
PROGRAM TABLE SET-UP	
Effective From Date: 12/01/2017	Effective To Date: 01/31/2019
Program Name: FFY2015 BJAG HEROIN/OPIOID	Program Short Name: 80004611
Program Code: **(MUST START WITH "F" followed by up to 9 characters) FJG1HEOP16**	Sub Account: 2016-DJ-BX-0653

FUNDING PROFILE - FUNDING LINE		
Draw Name:	Customer ID	Payment System Code – **Check one option only**
EDCAPS:	VC7000000001	**__D**
ECHO:	VC7000000002	**__E**
LOCES:	VC7000000003	**__L**
SMARTLINK:	VC7000000004	**__S**
ASAP- OTHER:	VC7000000005	**__Y**
ASAP:	VC7000000006	**__Z**
GRANT- NON DRAW:	VC7000000007	**__X__ No Code**

FUNDING IDENTIFICATION	
Federal Catalog Agency: (2 digit code) 16	Federal Catalog Suffix: (3 digit code) **738**
Letter of Credit No.: 1504 1240	

Authorized Signatory Seller/Child Department: _____ Date:_____ Name: _____.

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM INSTRUCTIONS

The Interdepartmental Service Agreement (ISA) Form is issued by the Office of the Comptroller (CTR) pursuant to 815 CMR 6.00 for use by all Commonwealth Departments. The ISA Instructions are provided to assist both Buyer/Parent and Seller/Child Commonwealth Departments with the interpretation and completion of the ISA Form and are incorporated by reference into the ISA. The ISA Form is the "Contract" that documents the business agreement (joint venture) between two Commonwealth departments within the Executive, Judicial and Legislative Branches of government. A Department must be recognized as a Department in the State Accounting System (hereinafter referred to as "MMARS") in order to transfer or receive funding under an ISA. The ISA must comply with funding language in any appropriation act funding the ISA, as well as all applicable general and special state or federal laws, regulations. The Buyer/Parent and Seller/Child are responsible for reviewing and complying with the applicable CTR policies (including but not limited to the ISA, electronic signature and state finance law policies) located at the CTR Knowledge Center under Procurement and Contracts and also at the CTR Website at: Comptroller Policies. While reasonable efforts have been made to assure the accuracy of the legal requirements for ISAs, Departments should consult with their legal counsel to ensure compliance with all legal requirements related to their performance under an ISA. PLEASE NOTE THAT NOT ALL APPLICABLE LAWS HAVE BEEN CITED IN THIS DOCUMENT. INSTRUCTIONS AND HYPERLINKS MAY BE ADDED OR CHANGED WITHOUT NOTICE, SO CHECK THIS DOCUMENT PERIODICALLY FOR UPDATES.

➔ MMARS DOCUMENT ID: Enter the state accounting system (MMARS) BGCN or BGCS or other authorized MMARS document number associated with this ISA. ISA related DOC ID Numbering must be done as described below. The Doc ID must be the Doc ID entered into MMARS and reflected on the supporting ISA paperwork. All ISA Doc IDs MUST START WITH "ISA", as follows:

EXAMPLE DOC ID Number: **ISA**EPS12345678SDF06A

First 3 Characters	Second 3 Characters	Next 8 Characters	Next 3 Characters	Next 2 Characters*	Last Character
ISA	Buyer/Parent Department Alpha	Buyer/Parent defined. May be numeric, alpha or combination	Seller/Child Department Alpha	Fiscal Year	A (initial document) B (1st Amendment) C (2nd Amendment)
ISA	EPS	12345678	SDF	06	A

➔ BUDGET FISCAL YEAR. Enter the Budget Fiscal Year of the ISA or ISA Amendment, as appropriate.

➔ REQUEST FOR RESPONSE REFERENCE NUMBER. If the Seller/Child responded to an RFR that was posted on Comm-PASS, enter the RFR Reference Number as posted. If an RFR was not used, indicate "N/A". Seller/Child Departments may respond to a Request for Response (RFR) or other solicitation of a Buyer/Parent Department. If the Seller/Child Department is selected as a contractor, the ISA Form must be used as the "contract" (instead of the applicable Commonwealth Terms and Conditions and Standard Contract Form and Instructions).

➔ BUYER/PARENT/SELLER/CHILD DEPARTMENT NAME: Enter the 3 Alpha MMARS Department Code. For Example "CTR" for the Office of the Comptroller.

➔ BUSINESS MAILING ADDRESS: Enter the address where all correspondence to the ISA Manager must be sent. Unless otherwise specified in the ISA, legal notice sent or received by the Department's ISA Manager (with confirmation of actual receipt) through the listed fax number(s) or electronic mail address for the ISA Manager will meet any requirements for written notice under the ISA.

➔ ISA MANAGER: Identify the authorized ISA Manager who will be responsible for managing the ISA. ISA Managers must be Department Head Authorized Signatories in order to execute the ISA and otherwise obligate the Department with the appropriate MMARS Security to support Department Head Signature Authorization.

➔ PHONE/FAX/E-MAIL ADDRESS: Identify the phone, fax number(s) and electronic mail (e-mail) address of the ISA Manager.

➔ PURPOSE OF ISA. Check off whether this is a new ISA or an ISA Amendment. For New ISAs, enter the total Maximum obligation for the duration of the ISA. If an ISA Amendment, check off any of the Amendments that are being made and complete any information in the blanks provided and the Attachments that are identified.

➔ BRIEF DESCRIPTION OF PERFORMANCE GOALS TO BE ACCOMPLISHED BY THIS ISA, OR IF AMENDMENT, IDENTIFY WHAT IS BEING AMENDED: Identify a brief description of the ISA, ISA name and performance to be accomplished under the ISA. If an ISA Amendment, identify what is being amended. Merely stating "see attached" or referencing attachments without a narrative description of performance is insufficient *and will result in ISA or Amendment being returned to MMARS Liaison of Buyer/Parent Department*. The description is used to specifically identify the ISA performance, match the ISA with attachments and determine if the appropriate process has been selected.

➔ INDICATE WHETHER SELLER/CHILD DEPARTMENT STATE EMPLOYEES (AA OBJECT CLASS) WILL BE FULLY OR PARTIALLY FUNDED UNDER THIS ISA. Justification for use of state employees and details of who will be working and work that will be performed must be included as part of ATTACHMENT A.

➔ ACCOUNT INFORMATION.

- Check the correct option for either a BGCN – non-subsidiarized (federal, capital, trust); BGCS – subsidiarized (budgetary); Other (CT, RPO or other document authorized by CTR); Non-Financial ISA (no funds are transferred from Buyer/Parent to Seller/Child with resources committed to ISA; or Amendment without Budget changes to ISA (used only for an Amendment if there are no changes to the budget and no changes to Attachments B and C (if applicable).
- Identify for each account under the ISA whether the account is "added", "deleted or "no change". **THIS SECTION MUST BE COMPLETED FOR AMENDMENTS EVEN IF THE ACCOUNT INFORMATION HAS NOT CHANGED.** Enter each ISA account, fund, major program code and program code for all funding under the ISA. Attachment B must be completed for all financial ISAs and ISA Amendments (with Budgetary or Account amendments). Attachment C must be completed for any financial ISAs or ISA Amendments with Budgetary or Account amendments involving federal or capital funds).

➔ ISA ANTICIPATED START DATE**.** Enter the anticipated start date, provided that the Seller/Child certifies that it will not incur any obligations related to this ISA prior to the date that this ISA is executed, NOR prior to the date that sufficient funding for the obligations under this ISA available in the Seller/Child account for expenditure.
Note - ISA Duration. ISAs can be executed for the duration that makes sense from a business perspective. Multi-Year ISAs are encouraged if it best supports the Buyer/Parent and Seller/Child business processes. Similar to other types of contracts, all ISAs are subject to appropriation or other available funding. Therefore, Departments can enter into a Multi-year ISA even if funding transactions have to be

processed annually to support each fiscal year of the ISA. Buyer/Parent and Seller/Child Departments are responsible for ensuring that the funding is in place in the authorized Seller/Child account(s) to ensure that the Seller/Child Department can timely encumber funds and pay employees, contractors, grantees, etc. from the authorized ISA Seller/Child account(s)in accordance with the ISA Terms and Conditions.

➔ TERMINATION DATE OF THIS ISA: The Buyer/Parent Department must enter the date the ISA will terminate. An ISA must be signed for the full duration and amount in accordance with what is negotiated between the Buyer/Parent and Seller/Child Department. Amendments to extend the termination date, such as renewals, must be made using the ISA Form and must be signed by authorized Department Head signatories (with appropriate MMARS Authorized Signatory Security roles) of both the Buyer/Parent and the Seller/Child Department contemporaneously with the need for the amendment but no later than the termination date (or as previously amended) in accordance with 815 CMR 6.00.

➔ AUTHORIZING SIGNATURE FOR BUYER/PARENT DEPARTMENT/DATE: The Authorized Buyer/Parent Department Signatory must, in their own handwriting, and in ink, sign AND enter the date the ISA is signed. **THE DATE IS AN INEXTRICABLE PART OF THE SIGNATURE AND MUST BE COMPLETED BY THE SIGNATORY AND MAY NOT BE PRE-FILLED OR ENTERED AFTER THE SIGNATURE BY ANOTHER PERSON.** Rubber stamps, typed or other images are not acceptable. See CTR policies on Electronic Signature and Department Head Signature Authorization for Department Head and Authorized Signatory certifications and responsibilities.

➔ NAME /TITLE: The Buyer/Parent and Seller/Child Department Authorized Signatory's name and title must appear legibly.
NOTE: Secretariat signoff is not required in order for CTR to process an ISA. However, Seller/Child and Buyer/Parent Departments are required to follow any internal secretariat procedures when obtaining authorization for an ISA (or for certain ISA transactions such as an inter-subsidiary transfer "TS") prior to submission to CTR. All ISAs are periodically reviewed by CTR to verify that the signatories are authorized by their Department Head to execute contracts. Departments are responsible for timely processing through secretariats to ensure timely funding as required under the Department Head certifications.

➔ **ATTACHMENT A – TERMS OF PERFORMANCE AND JUSTIFICATIONS.** ***Attachment A is required for all new ISAs and for all ISA Amendments.*** Departments must use this attachment and insert (type, or copy and paste) the required information in addition to other terms of performance negotiated by the parties under Section 9. Sections 1-8 are mandatory and must be answered in detail or the ISA will be returned to the Buyer/Parent Department MMARS Liaison. All information must be inserted into Attachment A using as many pages as necessary. If Amending the ISA, completion of Sections 1, 2 and 3 identifying what is being amended and the reasons for the amendments is required. For sections 4-9 enter only the amended language in the sections being amended.

➔ **ATTACHMENT B - ANTICIPATED BUDGET.** ***Attachment B is required for all New ISAs and for all ISA Amendments with budget and accounting transactions.*** Departments must use this form. Insert all required information and use as many additional lines and pages as necessary. This attachment must breakdown the specifics of the ISA funding, by fiscal year, Seller/Child account, object class, description and amount. For multi-year ISAs the Attachment must provide a subtotal each fiscal year of the ISA (which equals each fiscal year's anticipated maximum obligation). All ISAs must provide a total maximum obligation for the total duration of the ISA (which must equal the total of all fiscal year subtotals) and must match the "Total Maximum Obligation for Duration of ISA" on the executed ISA.

- Check "Initial ISA Budget" , or "ISA Amendment"
- Identify the MMARS Doc ID if the ISA is being amended.
- **Complete Columns A-E For New ISAs. Complete Columns A-I for Amendments.**
  - **Column "A" (Budget Fiscal Year).** Enter the fiscal year of the funding, or amendment. For Multi year ISAs Column A must list planned expenditures by each fiscal year of the ISA.
  - **Column "B" (Seller/Child Account).** Enter the number of each Seller/Child account listed on the ISA Form. For ISAs using multiple Seller/Child Accounts, Column B must list planned expenditures for each Seller/Child account.
  - **Column "C" (Object Class).** Enter the Object Class (subsidiary) as outlined in the CTR Expenditure Classification Handbook (for example, "AA" for Employee compensation, "EE" for Administrative Expenses, "HH" for Consultant Contracts, etc.). IF the line item is authorized for multiple fiscal years, enter a separate line-item for each fiscal year of the ISA in which the line-item is authorized, specifying the estimated amount of the authorized expenditure. Line-items break downs of estimated expenditures by Object Class are required even if the Buyer/Parent account is non-subsidiarized, since the Budget acts as the authorization for the ISA expenditures. For subsequent fiscal years, entering "Balance Forward Amount" for federal, bond and trust accounts is insufficient, since good project management practices presume that departments will be managing estimated expenditures over the life of a project with planned fiscal year obligations, rather than managing projects solely based upon remaining uncommitted estimated receipts or uncommitted balances.
  - **Column "D" (Description).** Enter a brief description of the type of authorized budget expenditure or category, (e.g., "Conference Materials", "Program Manager", "Health Evaluations" etc.)
  - **Column "E" (Initial ISA Amount/or Amount Prior to Amendment).** Enter the amount for the budget item authorized under the ISA for each fiscal year. If the ISA is being amended, enter the current amount for this line-item, prior to the amendment. The Amendment amount will be entered in Column G and the new total will be entered in Column I.
  - **Column "F" (+/-)** is only used if the ISA is being amended to add or reduce a budget line item. Enter "+" for budget addition or "-" for a budget reduction.
  - **Column "G" Amendment Amount** is only used if the ISA is being amended to add or reduce a budget line item. Enter the amount of the budget line being increased or decreased.
  - **Column "H" (Carry-In)** is only used if the ISA is being amended to reduce a prior year federal grants fund line item with uncommitted estimated receipts that are being re-authorized in the current or a future fiscal year. Enter "YES" in this column for each line item being amended (by object class and description) to reflect a reduction in the budget in a prior fiscal year line item, and for each line item being added (by object class and description) to reflect a reauthorization of the funds in the current or a future fiscal year.
  - **Column "I" New Amount After Amendment** is only used if the ISA is being amended to add or reduce a budget line item. Enter new ISA Amount after the adding or reduction of the line-item amount referenced in Column G.
- FISCAL YEAR SUBTOTALS AND TOTAL MAXIMUM OBLIGATION.

- Fiscal Year Subtotals. For single fiscal year ISAs enter the fiscal year (e.g., "Fiscal Year 2007") and enter the subtotal of all "Current Amounts" (Column E) for that fiscal year. For Multi-year ISAs, enter each fiscal year of the ISA as a separate subtotal and enter the subtotal of all "Current Amounts" for each fiscal year.
- Total Maximum Obligation for Duration of ISA. Enter the Total Maximum Obligation for the Duration ISA for all fiscal years (as identified on the executed ISA Form). For single fiscal year ISAs, this amount should be the same as the Fiscal Year Subtotal. For Multi-fiscal year ISAs, this amount should equal the total of all the listed fiscal year subtotals.

➔ **ATTACHMENT C – FEDERAL GRANT SELLER/CHILD ACCOUNT** (complete only if Buyer/Parent Account is a Federal Account). Please enter the following information on this form.

- Enter whether this is a "New" ISA or an ISA Amendment and enter the Budget fiscal year.
- Enter the Buyer/Parent and Seller/Child Departments, which must match the ISA.
- *Skip the Revenue Budget and Revenue Source which will be completed by CTR.*
- CENTRAL BUDGET STRUCTURE*:*
  - Appropriation Number. Enter the Appropriation Number assigned by ANF.
  - Payroll Indicator. Enter a Payroll indicator of Yes or No.
  - Estimated Budgetary Receipts. Enter the amount of the Estimated Budgetary Receipts (the amount estimated in the ISA or Amendment for the current state fiscal year).
  - BGCN Document Identification No. Enter the MMARS Document Identification Number for the Central Expense Document (BGCN). The BGCN must be entered and submitted to PEND in MMARS. Providing a screen print of the BGCN aids CTR in the processing of the ISA and set up of the accounts or account changes.
- COST ACCOUNTING STRUCTURE.
  - Total Maximum Obligation of ISA or ISA Amendment Amount. For New ISAs, enter the Total Maximum Obligation of the ISA for the full duration of the ISA. For ISA Amendments, enter the amount of the modification.
  - BGRG Document Identification No. Enter the MMARS Document Identification Number for the Reimbursable Grant Budget Document (BGRG). The BGRG must be entered and submitted to PEND in MMARS. Providing a screen print of the BGRG aids CTR in the processing of the ISA and set up of the accounts or account changes.
- MAJOR PROGRAM TABLE SET-UP. This sets up the cost accounting hierarchy with groups of activities (programs) all part of one structure. For example – a major program could be wastewater management – WASTE. All documents (contracts, encumbrances, payments will reference this code.) All documents (contracts, encumbrances, payments will reference this code.)
  - Major Program. Enter the 6 (or fewer) character Major Program Code assigned by the department.
  - Major Program Name. Enter the full Major Program Name.
  - Major Program Short Name. Enter the Major Program Short Name.
- PROGRAM PERIOD TABLE SET-UP OR EXTENDED PROGRAM PERIOD (EPP). Enter the Program Period or Extended Program Period (EPP) information. This establishes the effective period of the grant. Please note that end dates are "hard edited" by the system, thus please take into account the accounts payable period for grants when establishing this date. Multiple periods allow for easy periodic reporting aligned to federal reporting dates. However, a Buyer/Parent department may choose to use 1 reporting period – EPP – that encompasses all dates. The downside of this method is that specific periodic federal reporting by the system is not achieved.
  - Enter the Program Effective From Date and Effective to Date.
  - Enter the Program Period or Extended Program Period (EPP) information.
  - Enter the Program Period Name, and Program Period Short Name.
- PROGRAM TABLE SET-UP.
  - Enter Program Name. For example a program could be for "storm water discharge".
  - Enter Program Short Name:
  - Program Code. Enter the 10 (or fewer) characters. All Federal Program codes must begin with the letter "**F"**. This is the second level of the cost accounting hierarchy. Programs are individual activities within a Major Program. Using the major program example, a program could be for storm water discharge – the program code would be "Fstormdis". All documents (Recurring Payment Order (RPO), payments will reference this code.)
  - The sub account must be the sub account in the award letter or the draw on the federal grant will fail. If a sub-account changes, this code must change.
- FUNDING PROFILE - Funding Line. This must be filled out properly – indicating the federal payment system to be used. If the wrong payment system is indicated, the draws on the federal grant will fail. Enter a check next to appropriate Payment System Code.
- FUNDING IDENTIFICATION.
  - Federal Catalog Agency Code. Enter the 2 digit Federal Catalog Agency code.
  - Federal Catalog Suffix. Enter the 3 digit Federal Catalog Suffix code from your award letter or contact the appropriate agency. This must align to the grant award. The proper grant identification information is a federal reporting requirement.
  - Letter of Credit No. Enter the Letter of Credit No. for this grant award.

COMPLETED ISAS SHOULD BE SUBMITTED FOR PROCESSING TO:

Office of the Comptroller, One Ashburton Place – 9th Floor, Attention: Accounts Payable Bureau, Contracts, Boston, MA 02108
CTR Helpline: **617-973-2468**

Department of State Police
General Order

Effective Date	Number
July 22, 2014	**TRF-11**

Subject

Automatic License Plate Recognition

Purpose

The purpose of this policy is to establish guidelines and procedures for the proper use and application of Automatic License Plate Recognition (ALPR) System.

Policy

The availability and use of ALPR System provide opportunities for the enhancement of law enforcement agencies' productivity, effectiveness, and protection of 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 ALPR System.

Definitions and Acronyms

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. ALPR System is configured as either fixed, mobile or portable.

Alert: A visual and/or auditory notice that is triggered when the ALPR System receives a potential hit on a license plate.

Alert Data: Information captured by an ALPR relating to a license plate that matches the license plate on a hot list.

ALPR Data: Scan files, alert data, and any other documents or data generated by, or obtained thorough, utilization of the ALPR System.

ALPR Data Query Logs: A record of a search or query of ALPR data.

Continued next page.

Subject	Number
Automatic License Plate Recognition	**TRF-11**

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, Be On Look Out (BOLO), Attempt To Locate (ATL), and Wanted or Missing Person broadcasts or bulletins in which a license plate number is included, or other license plate numbers of interest entered by the Department or an authorized officer.

Hot List Download: The method by which the hot list data is transferred to a computer within a law enforcement vehicle.

Optical Character Recognition (OCR): The technology that supports the automated reading and digitizing of images of license plates that are captured by the ALPR System.

ALPR Administrator

The 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 be responsible for the following:

- Ensuring the proper selection of the personnel approved to operate the ALPR System and maintaining an adequate number of trained and authorized users;
- Authorize any requests for ALPR System use or data access according to Department policy;
- 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.

The ALPR Administrator shall:

1. Designate users who have been properly trained in the use and operational protocols of the ALPR System;
2. Allow access to the ALPR System for those users with an approved login and password; and
3. Ensure that any changes in hardware, software, policy, or law are the subject of continuing in-service training or bulletins.

Subject	Number
Automatic License Plate Recognition	**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 purpose;
- 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 be cleaned and maintained according to the manufacturer's recommendations; and
- Notify the ALPR Administrator of any malfunctions.

ALPR Alerts/Hits

The member shall prior to initiation of a stop based on a ALPR Hit or Alert:

- Visually verify that the vehicle plate number matches the plate number run by the ALPR System, including both:
  1. Alphanumeric characters of the license plate; and
  2. The state of issue.
- Verify the current status of the plate through:
  1. The Commonwealth's Criminal Justice Information System(CJIS), or
  2. National Crime Information Center (NCIC), or
  3. Department's Records Management System(RMS), or
  4. Other appropriate source of data, when circumstances allow, or as soon as practicable.

Manual Entry of Data

Manual entries may include, but should not be limited to:

- AMBER Alerts;
- Missing Child Alerts;
- Missing College Student Bulletins;
- Be On Look Out (BOLO);
- Attempt To Locate (ATL); or
- Wanted or Missing Person broadcast or bulletin in which a license plate number is included.

Continued next page.

Subject	Number
Automatic License Plate Recognition	**TRF-11**

Manual Entry of Data (Continued)

Manual entries entered into the ALPR System shall be:

- Manually updated when the information changes or is no longer current; and
- Documented with the specific reason by the member.

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.

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 be responsible for:

- The annual review of this policy and the procedures contained herein; and
- Making recommendations through channels to the Colonel/Superintendent or designee, for any necessary amendments.

As use of the technology progresses, the Department shall continue to monitor and assess the appropriateness of this policy, as with new technology may raise both legal and technological issues.

References

Executive Office of Public Safety and Security (EOPSS)- *The Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy*

Promulgated By:

Massachusetts State Police
Traffic Safety Resource Prosecutor FY 2017
Proposal to the Highway Safety Division
October 1, 2016– September 30, 2017

Executive Summary

The Massachusetts State Police, Traffic Programs Section ("Traffic Programs") is primarily responsible for the public education and implementation of the department's highway safety enforcement initiatives. Traffic Programs handles sobriety checkpoints, saturation patrols, Automatic License Plate Readers (ALPR), maintain and update all corresponding guidelines and regulations as well as, provide training for all troopers on related issues.

Additionally in 2008, the Commonwealth of Massachusetts enacted legislation that decriminalized the possession of certain amounts of marijuana. As an indirect consequence of the legislation, the public perception was such that the consumption of marijuana while operating a motor vehicle was permissible. In 2012, further expansion of the utilization of marijuana for medicinal purposes was approved by the voters, thus more motorists have been utilizing marijuana while operating a motor vehicle. NHTSA notes that, for fatally injured drivers, cannabis is detected in 7% to 37% with a mean of 14%. Once again in November 2016, voters passed a ballot initiative allowing for the use of recreational marijuana along with the right to grow and possess limited quantities. This law went into effect on December 15, 2016. As a result of the dramatic change in the law in regards to marijuana there is a need for increased police training, in every area of the law including: roadside stops, search and seizure, exit orders, citations versus charging, sobriety checkpoints, forfeiture, report writing and trial testimony. In addition, there is an immediate need for interpretation of the new laws and crafting of training materials on a daily basis. This new law has put a tremendous strain on the Massachusetts State Police, Traffic Programs, as well as the Standards and Training Section at the State Police Academy, as neither has a full-time staff attorney assigned to assist with education and training.

The National Highway Traffic Safety Administration's (NHTSA's) 2013-2014 National Roadside Survey found that more than 22 percent of drivers tested positive for illegal, prescription or over-the-counter drugs. This was true for both weekday daytime and weekend nighttime drivers. But illegal drug use increased from daytime to nighttime while use of prescription drugs decreased. By comparison, 1.1 percent of drivers tested positive for alcohol during the daytime on weekdays, but 8.3 percent of drivers on weekend nights tested positive (NHTSA).

Traffic Programs conducts, on average, over eighty checkpoints and saturation patrols annually. Troopers working these checkpoints are observing a marked increase in the use of marijuana by operators that proceed into the checkpoints. Troopers screening potentially drug impaired operators rely on academy training, field training and advanced training (ARIDE, DRE), however, unlike a preliminary breath test (PBT) which is used roadside as the last field sobriety test for alcohol, there is currently not a device available to screen for drugs. The Department of State Police is working in conjunction with Alere to create a roadside oral fluids drug testing pilot program with the ultimate

To assist in maneuvering through the advancements in technology and the law, the Massachusetts State Police are seeking funding for a Traffic Safety Resource Prosecutor (TSRP) to be assigned to the Traffic Programs section. This TSRP will provide law enforcement officers and their partners with training and resources in the area of vehicular crimes, assist with the Oral Fluids Pilot Program including reviewing all cases and preparing a legal challenge in court, assist prosecutors and law enforcement officers across the state with legal challenges to the sobriety checkpoints, and assist and navigate the legal challenges to the ALPR data as that program gets up and running and train law enforcement across the state in areas of distracted driving, drugged driving, ALPR, report writing and various other traffic related topics. These grant funds will ensure that as Traffic Programs navigates through these uncharted technological advances in the law enforcement field, the TSRP will be there to assist and guide through the successful process.

Statement of Need

In 2015 there were 344 fatalities on the Roadways of the Commonwealth, according to the *National Highway Traffic Safety Administration.* Many of these 344 incidents resulted in criminal charges. In that same year in Massachusetts, there were over 16,000 arrests for operating under the influence of alcohol or drugs. The Massachusetts State Police seeks to improve the ability of the Traffic Program to effectively conduct motor vehicle stops and arrests through education, training and legal guidance particularly focused on the following areas:

a. Vehicular crashes involving personal injuries
b. Operating under the influence of alcohol or drugs
c. Operating with a suspended or revoked license
d. Distracted driving
e. Medical Marijuana
f. Sobriety Checkpoints
g. Anticipated challenges to ALPR once warrants are written based on ALPR data.

Currently, Traffic Programs lacks the resources necessary to provide continuous, progressive training so that all law enforcement officers are trained to properly effectuate motor vehicle stops, write and serve warrants and effectively prepare a case for prosecution. Additionally, the whole law enforcement community is also in need of training and all partners could benefit from consistent, up-to-date reference materials to assist in the adjudication of these issues.

Goal

To reduce fatalities, injuries and economic losses resulting from motor vehicle crashes on the roadways of the Commonwealth of Massachusetts by providing training, education and technical support to law enforcement officers and other traffic safety partners throughout the state.

Objectives

1. To have one full-time staff attorney assigned to Traffic Programs dedicated exclusively to training, educating and offering technical support to law enforcement officers throughout the state.
2. To assist and navigate the legal challenges to sobriety checkpoints, oral fluid drug testing and ALPRs in criminal investigations and prosecutions.
3. To develop curriculum in all areas of traffic safety.
4. To develop and update traffic safety programs and resources.
5. To act as a resource for all traffic safety partners across Massachusetts.

6. To participate in working groups and subcommittees on traffic safety.

FFY 2017 Program Plan

The Massachusetts State Police seek to hire an individual who is a former prosecutor who will provide training, education and technical support to our Traffic Programs Section. Traffic crimes and safety issues include but are not limited to: alcohol and/or drug impaired driving, vehicular homicide, occupant restraint and other highway safety issues. The TSRP will assess the needs and demands unique to Massachusetts and work in conjunction with many agencies to meet these needs. The National Highway Traffic Safety Administration (NHTSA), Municipal Police Training Committee, Mass. Chiefs Association, crime laboratory, and victim advocate groups will all be utilized to facilitate services to both prosecutors and law enforcement.

Qualifications:

- Juris Doctorate with at a minimum of eight years prosecuting criminal cases.
- Member in good standing of the State Bar.
- Extensive experience in the prosecution of impaired driving cases.
- Knowledge about the NHTSA Standardized Field Sobriety Testing, sobriety checkpoints and saturation patrols, and the Drug Evaluation Program.
- Impressive writing and oral advocacy skills.
- At least three years of training experience.
-

Budget Narrative

Personnel

- **Traffic Safety Resource Prosecutor – October 1, 2016 – September 30, 2017**

  In order to get an attorney with the experience and necessary to take on the challenges in Traffic Programs, we request a salary commiserate with the level of experience required to fill this TSRP position.

Fulltime Staff Attorney Salary:	**$110,000.00**
Additional Salary costs for Staff Attorney:	**$51,502.00**
Fringe and Insurance (FY 2017 rate 35.16%)	$38,676.00
Payroll Tax Rate (FY2017 rate 1.66%)	$1,826.00
Indirect (FY 2017 rate 10.00%)	$11,000.00
Total Personnel Expense (HSD figures)	**161,502.00**
Total Personnel Expense	***161,502.00***

Office Supplies/Miscellaneous

- **Office Supplies/Equipment Fees/Misc – October 1, 2016 – September 30, 2017**
  Office supplies, equipment fees, and miscellaneous items associated with the implementation of the outlined grant activities and projects including: staff attorney bar dues, printing, training supplies, traffic safety training equipment, desk calendar, disks, memory sticks, audio-visual equipment, as well as other items as needed.

Cost: $ 5,498.00

Total Office Supplies/Equipment/Miscellaneous ***$5,498.00***

Travel/Trainings and Conferences

- **Drugged Driving – Fall 2017**
  The TSRP will host a one-day training on *Identifying the Drugged Driving* for prosecutors and law enforcement officers. This training will focus on marijuana and how to identify the signs and symptoms of marijuana impairment. This training will incorporate a section on drug recognition utilizing the experienced DREs in the Commonwealth.

  Cost: $ 0.00

- **Cops In Court – Fall 2016/Summer 2017**
  The foundation to any successful Operating Under the Influence prosecution is a well written police report. This is an area of weakness for many law enforcement officers as it is a skill that is rarely taught in any class. National Traffic Law Center's *Cops In Court* course will be utilized to train Massachusetts law enforcement officers. This training will be repeated a least two times.

  Cost: $ 0.00

- **NHTSA TSRP Regional Training – Winter 2017**
  Biannually NHTSA sponsors regional meetings that bring together the TSRPs from Vermont, Maine, New Hampshire, Rhode Island, Connecticut, and Massachusetts. These meetings are extremely valuable for the brainstorming and exchange of ideas to increase public awareness of the NHTSA campaigns.

  Cost: $200.00

- **The 22nd Annual IACP DRE Section's Training Conference on Drugs, Alcohol, and Impaired Driving – Summer 2017**
  IACP DRE Section's Annual Training Conference on Drugs, Alcohol and Impaired Driving, has helped DREs and other health and safety professionals stay up-to-date on drug trends, legal issues, and innovative technology. Most TSRPs from across the country attend this training to get up to date information on the drug trends and new technology. The 2017 conference will be held in Maryland 2017.

  Cost: $2,000.00

- **Lifesavers Meeting – April 3 – 5, 2016 – Spring 2017**
  Lifesavers is the premier national highway safety meeting in the United States dedicated to reducing the tragic toll of deaths and injuries on our nation's roadways. Drawing over 1,500 participants in 2015, Lifesavers continues to be the essential conference since its start in the early 1980s. Each year, the Lifesavers Conference provides a forum that delivers relevant and timely common-sense solutions to today's critical highway safety problems. The 2017 meeting will be held in Charlotte, NC on April 2017.

Cost: $2,000.00

- **Overtime for Sobriety Checkpoint Attendance – October 1, 2016 – September 30, 2017**
  The TSRP will be required to assist with sobriety checkpoints as the new oral fluid drug testing program gets under way. This category will cover overtime pay for the TSRP to assist with at least ten checkpoints throughout the calendar year.

  Cost: $8,000.00

- **In-State Travel– October 1, 2016 – September 30, 2017**
  This category covers in-state travel (mileage, tolls and parking) associated with the implementation of the outlined grant activities and projects and any additional training opportunities with law enforcement or other traffic safety agencies.

  Cost: $800.00

Total Travel/Trainings and Conferences Expense ***$13,000.00***

Project Evaluation

The success of the Massachusetts State Police's initiatives will be evaluated in the following manner:

Evaluation Forms: At each formal training and/or conference, the State Police provides all attendees with an electronic evaluation form. The evaluation forms are tailored for the specific event, but are standardized in that the attendee is always asked to evaluate the content of the presentation, the practical application of the material in a courtroom setting, and the usefulness of any training materials. In addition, the attendee is provided with several open-ended questions that invite recommendations for ways in which the event can be improved along with any additional feedback.

Technical Assistance: The TSRP will log the number of technical assistance calls that come in from the law enforcement community and other partners and report that number in an annual report.

The Success of the Oral Fluid Drug Testing Program: The TSRP will monitor and guide the oral fluid drug testing program as it gets underway lending legal advice and assistance when necessary to make this program as successful and useful to Massachusetts as possible.

Challenges to the Sobriety Checkpoints: There are currently numerous challenges to the sobriety checkpoints to both the State Police paperwork that guides the checkpoints as well as the administration of the checkpoint itself. The TSRP will assist both the law enforcement officers and prosecutors in responding to these challenges and report the number of successes.

Partners

The State Police partners include: The International Association of Chiefs of Police, Mothers Against Drunk Driving, The Brain Injury Association, Mental Health and Substance Abuse Corporations of Massachusetts, Inc., The Department of Public Health, The Massachusetts District Attorneys

Association, The Municipal Police Training Committee, and The Judicial Institute. The State Police do not receive funding for a TSRP from any other sources.

Supplanting

The TSRP position will be developed and maintained with the use of HSD grant funding. No funds will go to pay for ongoing activities already budgeted or for activities assigned to a position.

HSD Grant Budget
FFY 2016
October 1, 2016 to September 30, 2017

Personnel - October 1, 2016 – September 30, 2017	
Staff Attorney	$110,000.00
Fringe Benefits for Staff Attorney (including taxes and insurance (35.15% + 1.66%)	$40,502.00
Indirect Costs of salary (10%)	$11,000.00
Total	**$161,502.00**
Total Personnel Expense:	***$161,502.00***

Office Supplies/ Equipment Fees/Miscellaneous – Fall 2016 - Spring 2017

Office Supplies/Equipment Fees/Misc. – October 1, 2016 – September 30, 2017
Office supplies, equipment fees, and miscellaneous items associated with the implementation of the outlined grant activities and projects including: staff attorney bar dues, printing, training supplies including optokinetic nystagmus drums, Turning Point response cards, desk calendar, disks, memory sticks, and audio-visual equipment, as well as other items as needed.

$5,498.00

Total Supplies/ Equipment/Misc. Expense: ***$5,498.00***

Travel, trainings and conferences

Drugged Driving Training – Fall 2016	
Conference handouts and supplies	$0.00
Cost:	**$0.00**
Cops In Court – Fall 2016 and Summer 2017	
Conference Handouts and supplies x 2	$0.00
Cost:	**$0.00**
NHTSA Regional Meetings – Winter 2016	
Mileage/parking	$200.00
Cost:	**$200.00**

The 22nd Annual IACP DRE Section's Training Conference on Drugs, Alcohol, and Impaired Driving – Summer 2017

Summer 2017 Meeting: August 2017- Maryland	
Airfare	$ 650.00
Mileage and airport parking	$ 179.00
Hotel (4 nights @ $189.00)	$ 756.00
Per diem (30 X 5)	$ 150.00
Registration fee:	$ 200.00
	$2,000.00
Cost:	**$2,000.00**

Lifesavers Conference – Spring 2017

Spring 2015 Meeting: April 2017, Charlotte, NC	
Airfare	$450.00
Mileage	$179.00
Hotel (4 nights @ $189.00)	$756.00
Per diem (43 X 5)	$215.00
Registration fee:	$400.00
	$2,000.00
Cost:	**$2,000.00**

Overtime for Sobriety Checkpoint Attendance – October 1, 2016 – September 30, 2017

TSRP	$8,000.00
Cost:	**$8,000.00**

In-State Travel – October 1, 2016 – September 30, 2017

Cost:	**$800.00**

Total Travel/Checkpoints/Training and Conferences:	***$13,000.00***

Total Proposal:	***$180,000.00***



Why Take Our Word For It?

Real-world case studies and examples of license plate recognition solving crimes and saving lives

Sacramento County Sheriff's Department Expands Facial Recognition Program to 500 Officers

LIVERMORE, CALIFORNIA (May 19, 2016) – Vigilant Solutions announces today that Sacramento County Sheriff's Department is expanding the use of its FaceSearch™ facial recognition solution to approximately 500 agency users based on its success over the past year in a pilot operation.

"We are deploying facial recognition to approximately 500 officers here at Sacramento County Sheriff's Department," states Sergeant Kyle Hoertsch. "Over the past year we have made as many as 35 criminal identifications resulting from its use. Two notable cases are the identification of a cold case homicide suspect on the first day of use, and the identification of another individual on a routine traffic stop. The gentleman was covered in prison tattoos, did not have a valid ID, and the name he provided to us included the name of a famous actor as the middle and last names. Upon taking his photo using the mobile app, we were returned a list of possible matches within about two seconds. Upon review of the possible matches, the officer on patrol was able to visually confirm that the gentleman was indeed the same person seen in a 2006 booking photo out of Ohio."

Sergeant Hoertsch continues, "One thing that we like about the system is that it doesn't consider skin tone in providing the possible matches. Unless the race is known and you enter it as a parameter into the search, the system will return possible matches based solely on the measurements of the face. It attempts to match these measurements against criminal image databases such as mugshots, registered sex offenders, and other sources like this; we are not comparing against non-criminal databases such as driver's license photographs. It's also important to note that the results returned by the system are possible matches only. It is only through officer review and evaluation of all of the available information that a positive identification can be made."

Roger Rodriguez, Manager of Image Analytics for Vigilant Solutions and world-renowned facial recognition expert, comments, "Having been to Sacramento County and met Sergeant Hoertsch, I see a lot of positive momentum in their facial recognition program. There are some definite parallels to what I encountered in creating the facial recognition unit within the NYPD's Real-Time Crime Center – redefining expectations from Hollywood's depiction of the technology, helping users understand how to make use of less-than-ideal suspect images, and many more. Sergeant Hoertsch and his team certainly understand these issues and are showing real results in leveraging the system to improve the agency's ability in making criminal identifications. He and his team are doing a great job, and we wish them well in their expansion."

About Vigilant Solutions:
Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Suspect in hit-and-run death of 9-year-old girl located using historical and commercial license plate reader data

LIVERMORE, CALIFORNIA (March 31, 2016) – Vigilant Solutions announces today that a state law enforcement agency used historical and commercially-available license plate reader data to locate and arrest a suspect in the fatal hit-and-run death of a 9-year-old-girl. Due to sensitivities involved with this case, the agency has requested that identifying details in the case not be released.

A 9-year-old girl was holding her mother's hand as they crossed the street when she was struck by a sport-utility vehicle turning into an intersection and into the path of the girl and her mother. Surveillance video shows the male driver of the vehicle exit the SUV, look at the little girl's body, and then return to the vehicle and leave the scene.

A spokesperson for the state agency comments, "A general description and partial license plate of the vehicle was provided to our agency from the local police department. Using this information, along with access to the state motor vehicle records, we were able to conduct a search of all vehicles matching these criteria. This information was forwarded over to the local police department working the case."

"A detective from the local police department advised us of a suspect license plate, which was included in the search results. Using the complete license plate number, we were then able to look into Vigilant's commercial LPR data as well as LPR data shared from neighboring agencies to provide images of the vehicle for visual verification by the mother and other eyewitnesses."

"Upon a confirmation that this vehicle did appear to be our suspect vehicle, and using historical LPR data, we were able to determine some possible locations for the vehicle. Using this information, the vehicle was successfully located, allowing the investigation to move forward. It was determined that the owner of the vehicle was allegedly a passenger at the time her boyfriend struck and killed the young girl. She had reported her vehicle stolen shortly after the accident, presumably in an effort to disassociate herself from the fatal accident. The driver's sister reported to the media that her brother was in the country illegally which may be why he panicked and fled the scene. The driver was charged with leaving the scene of a fatal accident, and owner of the vehicle was charged with hindering apprehension."

Brian Shockley, Vice President of Marketing for Vigilant Solutions, adds, "Thank you to all involved in helping solve this tragic case. It is very concerning that despite the many successes of the technology, the fact that the data is anonymous, and the fact that a federal law already exists to protect driver's privacy, that pending legislation in several nearby states - if passed - would prohibit these types of investigations from ever taking place. Some of these proposed laws require the immediate disposal of LPR data unless it is part of an active investigation. These proposed laws also limit law enforcement's access to lawfully-obtained and commercially available LPR data – data that is helping to solve all types of crimes, locate missing persons, and even exonerate individuals. We applaud the many agencies out there that are sharing success stories like this to help lawmakers and the public understand how LPR is a critical law enforcement tool that improves officer safety and provides for safer communities."

About Vigilant Solutions:

Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:

Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Historical license plate reader data used by Lee's Summit Police Department to locate homicide suspect

LIVERMORE, CALIFORNIA (February 11, 2016) – Vigilant Solutions announces today that its license plate recognition (LPR) cameras and commercial LPR data are being used by Lee's Summit Police Department to improve safety for its residents, including the recent location and arrest of a homicide suspect.

Located in the metropolitan area of Kansas City, Lee's Summit covers around 65 square miles and is home to roughly 100,000 residents. Lee's Summit Police Department has a single mobile license plate reader system and also leverages Vigilant's network of commercially available LPR data to supplement its own data for investigative purposes.

Detective and Criminal Intelligence Officer Mark Phillips manages the agency's LPR program. Detective Phillips explains, "The system is incredibly valuable in helping locate vehicles of interest. In 2015 alone, we recovered 101 stolen vehicles with the use of our LPR system, some of which resulted in arrests. While it is nice to return stolen vehicles to their owners, this is not the only reason we look for these vehicles. Stolen vehicles are often used to perpetrate other, more serious, crimes. It is important to locate these vehicles as soon as possible in order to improve the chances of returning the vehicle to its owner and to reduce the likelihood that a more serious crime may occur that may endanger our citizens or officers. Considering that the system was only in use for roughly nine months last year, these are extremely impressive results, equating roughly to a vehicle recovery every 2.5 days."

Vigilant's commercial data network adds roughly 36,000 monthly LPR detections in Lee's Summit and almost one million monthly LPR detections in the surrounding Kansas City metro area; this is in addition to any data collected by the agency's system. All LPR data is anonymous in nature and does not contain information on drivers or registered owners. Connecting an anonymous license plate number to a registered owner is done only with a permissible purpose as defined by the federal Driver's Privacy Protection Act (DPPA), and this does not occur within the Vigilant Solutions system.

Detective Phillips concludes, "The historical LPR data offered by Vigilant has proven valuable in a number of investigations here in Lee's Summit. For example, last summer the data was useful in locating and arresting a dangerous homicide suspect. We had a license plate number for the suspect's vehicle. We searched the historical LPR data for this vehicle and found very limited data in the prior 30 days. But, because of several detections dating back several months, we were able to focus our search efforts around a certain location in Kansas City. With this information, we were able to locate the suspect's vehicle and establish surveillance which ultimately led to this individual's apprehension and arrest by members of Kansas City Police, Federal Marshals, and ATF. Our community is certainly a safer place with this individual off the street."

About Vigilant Solutions:

Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:

Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

License plate reader and historical license plate reader data used in homicide investigation

LIVERMORE, CALIFORNIA (February 9, 2016) – Vigilant Solutions announces today that an agency used its Vigilant Solutions mobile license plate reader (LPR) to develop a lead in a difficult homicide case. The agency then used Vigilant's historical and commercially available LPR data to locate the suspect vehicle. Due to the ongoing investigation, the agency name and certain details of the case have been omitted at the agency's request.

A spokesperson for the agency explains, "Our victim was found deceased at an intersection here in the City. He had suffered a severe brain injury from a fractured skull. The investigation revealed that the victim did not know anyone in the immediate neighborhood, and our homicide detectives did not know how he arrived at this location. Interviews with family members revealed that he was last seen alive at his home on the prior day. The victim's vehicle was missing from his residence."

"Investigators queried the victim's license plate number in Vigilant's LEARN system and quickly determined that one of our patrol vehicles equipped with a Vigilant LPR system scanned the victim's plate only hours before the homicide in the downtown entertainment district less than two miles from where the body was found."

"The victim's vehicle was located and searched for any evidence that may assist in the case. Locating the victim's vehicle also allowed investigators to obtain video from surrounding surveillance cameras which showed the victim walking into and out of a nearby bar. A further search of surveillance video allowed investigators to obtain images of the victim being placed into another vehicle and leave the area. It was believed that this vehicle transported him to the area where his deceased body was found."

"The suspect vehicle was eventually identified, and investigators used Vigilant's historical LPR data to obtain previously scanned images of the suspect vehicle for comparison to the images captured on the city surveillance video from the night of the homicide. During the comparison, investigators were able to see some identifying characteristics on the vehicle which helped confirm it was the correct vehicle. Using the historical LPR data also provided investigators with information on where to best locate the suspect vehicle. Two suspects were identified in the homicide, and the investigation is ongoing."

Tom Joyce, Vice President of Product Development for Vigilant Solutions and retired Cold Case Commander from NYPD, comments, "This is a textbook example of solid investigative work on the part of the agency to use anonymous data sources like LPR and surveillance video to develop leads. We applaud the agency and wish them well in bringing the responsible individuals to justice."

About Vigilant Solutions:

Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:

Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Grosse Ile Police Department Exonerates Two Individuals Using Fixed License Plate Reader Cameras

LIVERMORE, CALIFORNIA (February 4, 2016) – Vigilant Solutions announces today Grosse Ile Police Department in Michigan used its fixed license plate reader (LPR) cameras to exonerate two individuals from wrongdoing.

Grosse Ile has Vigilant Solutions fixed license plate reader cameras monitoring one of the bridges to the island community to enhance the safety of its citizens. Based on recent successes, they are in the process of adding additional fixed LPR cameras to cover the other bridge onto the island.

Lieutenant Robert Bow of Grosse Ile PD explains two separate cases in which the cameras were used to exonerate individuals from false accusations, "In the first instance, a woman had accused her ex-husband of vandalizing her vehicle. Upon questioning the suspect, he informed us that he had not been on the island during the time of the reported incident. We began investigating his alibi, and the data from the license plate reader cameras helped to support his claim. Upon querying his license plate in our system, we were able to confirm that his vehicle was not on the island at the time of the crime. This data allowed investigators to focus on other suspects, and ultimately solve the case."

"In another case, we had someone call the department claiming that a friend had held him at gunpoint and threatened him. The suspect denied the incident, and stated that he not been on the island at the time of the reported incident. Upon checking the LPR system, we were able to find data that supported this alibi. We then questioned the complainant on his accusation, at which point, he confessed to filing a false report in hopes of getting his friend in trouble."

Lieutenant Bow concludes, "It is important to note that the LPR system is unable to place an individual in a vehicle – it is anonymous in nature and only provides us with data points on the vehicle's location. Because of this, the LPR data was not sufficient by itself to exonerate these individuals. But, this data allowed investigators to better focus their efforts and exonerate these individuals and arrive at the truth."

About Vigilant Solutions:

Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:

Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Joplin Police Solve Two Hit-and-Run Cases with Assistance from Vigilant Solutions License Plate Reader Data

LIVERMORE, CALIFORNIA (February 3, 2016) – Vigilant Solutions announces today that the Joplin Police Department in Missouri solved two recent hit-and-run cases with the assistance of license plate reader (LPR) data from Vigilant Solutions.

Officer Brian Wenberg explains, "I was assigned a hit-and-run case in which the victim was walking out of a convenience store and witnessed an elderly male back out of a parking space next to his vehicle, striking his vehicle and leaving the scene. In his statement he noticed that the suspect was not wearing shoes when he left the convenience store. He believed the minivan was gold and stated that the first three letters of the Missouri license plate were SJ3. There was no other information provided."

"I spoke with the manager of the store and was told that the security cameras were not working at the time so there was no video. I ran the partial tag through all of our local systems and received no likely matches. I then did a partial plate search using Vigilant Solutions' LEARN. In reviewing the possible matches, I found only one gold minivan matching the partial plate."

"I drove to the apartment building where the vehicle had been scanned and found it. It had damage consistent with the victim's statement. Through further investigation and upon speaking to the property manager and the suspect's son, I learned that the suspect was recently admitted to a care facility due to his declining health. The son reported that his father's feet were too swollen to get his shoes on, and he had no clue his father had been involved in an accident. The commercially available LPR data in LEARN allowed me to solve this case, allowing the victim to receive insurance compensation and assisting the family of the elderly man to better understand the risks associated with him driving an automobile."

"In another recent case, a woman was waiting to make a right turn when a gold Chevy Cavalier ran into the driver's side rear of her car. She said the white male driver with shaggy black hair sped away. Her passenger believed the Missouri license plate on the suspect car to be either 6K9Z91 or 6K9Z81."

"Neither of these plates matched the alphanumeric format for Missouri license plates, but this was the only information available from the witness. Using LEARN and Vigilant's available commercial LPR data, I ran several partial plate searches and found only one viable match on a gold Cavalier. With the full tag number, and a permissible purpose under the Driver's Privacy Protection Act, I ran the tag through the state's Department of Motor Vehicles database which gave me a registered owner and address. After some investigation, we were able to locate and speak to the owner of the vehicle, who confessed to leaving the scene of a motor vehicle accident. Without the historical LPR data from Vigilant, this case would most likely have been closed as inactive and remain unsolved."

About Vigilant Solutions:

Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:

Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

21st Judicial District Drug Task Force Delivers Suspect in Cold Case Homicide Using License Plate Reader System

LIVERMORE, CALIFORNIA (February 1, 2016) – Vigilant Solutions announces today that the 21st Judicial District Drug Task Force in Tennessee used its license plate reader (LPR) system from Vigilant Solutions to bring to justice a suspect in a cold case homicide from 2002.

Scott Jones, Agent in Charge, explains, "Here at the 21st Judicial District Drug Task Force, we leverage our LPR systems for interdiction and drug enforcement efforts in the busy corridor along I-40 in Middle Tennessee. While the system has been very effective in helping us take drugs off the street and disrupt trafficking efforts, it can also deliver many other benefits as it did for me last September."

"I was working the Westbound side of I-40, and received an alert on a stolen vehicle – my second in two days. While we make arrests on stolen vehicles and other crimes, the primary goal of our task force in making a traffic stop is to look for vehicles that may be involved in narcotics trafficking. This particular vehicle was an older model pickup truck, and was being driven by an older gentleman. Based on my experience and training in drug interdiction, it was unlikely that this person was involved in trafficking. Had I not received the alert on the stolen vehicle from the LPR system, I would not have paid any attention to this vehicle. It is unlikely that anyone in law enforcement would have given this vehicle a second look."

"I proceeded with the traffic stop asking the gentleman if he knew the vehicle he was driving had been reported stolen. To my surprise, he responded that he knew it was stolen and that he had stolen it! He stated that he had witnessed the owner park the truck and leave the keys in the vehicle. Upon further questioning and investigation, this gentleman was identified as Lawton McNutt, and he had been recently released from prison for an attempted 1st degree murder. He was in possession of a firearm when taken into custody."

Agent Jones continues, "Mr. McNutt was taken to Hickman County Jail and booked in, at which point his fingerprints were ran through the Automated Fingerprint Identification System (AFIS) which had recently undergone an update to include some data from cold case files. The system indicated that he was a high probability match on a partial print obtained from a homicide scene in Wilson County in 2002. At this point, the Tennessee Bureau of Investigation (TBI) got involved, and Mr. McNutt has just been formally charged in the 2002 shooting death of 82-year-old James Hill."

Brian Shockley, Vice President of Marketing, comments, "We applaud the 21st Judicial Drug Task Force for being vigilant in their efforts to identify and interdict drug traffickers here in the state as well as using the system to bring this dangerous individual to justice."

About Vigilant Solutions:

Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:

Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Vigilant Solutions Recognized by Long Beach Police Department for Assistance in Infant Homicide Case

LIVERMORE, CALIFORNIA (November 12, 2015) – Vigilant Solutions announces today that it was recognized publicly at the recent International Association of Chiefs of Police (IACP) Conference in Chicago by the Long Beach Police Department for its assistance in a tragic case involving the murder of a three-week old infant.

Deputy Chief David Hendricks and Lieutenant Lloyd Cox presented a certificate to Vigilant's Founder and President, Shawn Smith, outlining some of the details of the case. On January 4, 2015, an attempted murder occurred in the 100 block of West 51st Street in the City of Long Beach. Three young adult victims were shot and a three-week old infant was kidnapped from the residence. Homicide detectives responded to the crime scene and identified the kidnapped infant as Eliza DeLaCruz. Detectives were determined to arrest the suspects responsible for the shooting and kidnapping, and worked tirelessly to find baby Eliza and return her to her family.

On January 5, 2015, the San Diego County Sheriff's Department notified detectives that the body of an infant was found in a trash dumpster in Imperial Beach, California. The medical examiner confirmed the identity of the infant as Eliza DeLaCruz.

Homicide detectives focused their efforts on solving the heinous and senseless murder of baby Eliza. Detectives had no suspect vehicle information and only a limited physical description of a single male suspect; therefore they could not even issue an Amber Alert to ask the public for help in the case. Detectives combed through the crime scene for evidence, interviewed witnesses and looked into the background of the shooting victims to determine a motive for the kidnapping and murder of baby Eliza.

Homicide detectives used every investigative tool available to them to gather evidence in the case, including License Plate Reader (LPR) technology, which can identify vehicles in or around a crime scene. However, the Long Beach PD's LPR data is limited to vehicles in the City of Long Beach, and the homicide investigation extended into Los Angeles, Orange, Riverside, and San Diego counties. Initially, detectives began making telephone calls to law enforcement agencies in each county to request assistance with their LPR data in researching possible suspect vehicle information. Detectives quickly realized this task was extremely time-consuming.

Homicide detectives learned that Vigilant Solutions maintains a national, commercial LPR database that is made available for law enforcement use. Detectives contacted Vigilant Solutions and explained the sensitive nature of the murder investigation. Vigilant Solutions immediately arranged for account profiles to be created and provided training to assist detectives in researching available LPR data to further their investigation. This data, and the analytic tools provided by Vigilant, proved essential in solving the murder of baby Eliza.

About Vigilant Solutions:

Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:

Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Vigilant Solutions Enables Over 217,000 Law Enforcement Data Sharing Relationships

LIVERMORE, CALIFORNIA (October 23, 2015) – Vigilant Solutions announces today that its hosted LEARN™ software enables 217,751 agency-to-agency license plate reader (LPR) data sharing relationships in the United States, enabling agencies to assist one another in solving all types of investigations. This data sharing network is the largest LPR data sharing network in the United States, if not the world.

The LEARN solution, hosted at a highly secure data center in Virginia, is limited to law enforcement use only. Featuring a variety of data protection standards such as CJIS-compliant access controls, case-level auditing, and account management at the agency level, LEARN is now used by over 1,000 agencies and 30,000 users. Law enforcement generated LPR data is managed by the agency generating the data, and agency managers may elect to freely share its LPR data with all agencies nationwide or with individual agencies at their discretion. Because the data is hosted, the data is never replicated or copied, leaving the agency in complete control of its data and preserving the integrity of the agency's data retention policy.

In addition to the over 217,000 data sharing relationships enabled, LEARN also enables agencies to share hotlists of vehicles of interest with one another. At present, there are over 17 million unique vehicles of interest being shared among law enforcement within LEARN, better enabling agencies to locate these vehicles by leveraging the LPR systems deployed around the United States within these agencies. While many of these LPR systems are Vigilant systems, Vigilant has also developed integrations with every major LPR provider, allowing agencies with legacy competitive equipment to benefit from the data sharing and investigative analytics available within LEARN.

Vice President of Marketing, Brian Shockley, explains, "In addition to the many successes that agencies have shared with us, these numbers are proof that LPR is an effective and valuable tool for fighting crime here in the United States. There is a great deal of talk in the media about license plate recognition systems. Much of this is focused on the question, 'Does LPR invade my privacy?' This question is often asked but rarely answered accurately. LPR is anonymous data – letters and numbers on a license plate. There is no information about a registered owner or other person captured by an LPR system. Further, a Federal law known as the Driver's Privacy Protection Act, or DPPA, requires that there be a permissible purpose under the law in order to look up a license plate in the Department of Motor Vehicles database to determine the registered owner. If there is an invasion of privacy then, quite simply, a Federal law is being broken and should be enforced."

"Putting that discussion aside, we would like to see the discussion shift toward recognizing the good that LPR technology does for society – solving cases, preventing crimes from occurring, improving officer safety and saving lives. When approved by the agency, we often publish success stories of how the technology aided in a case or helped to apprehend a dangerous individual. While we get many of these, they do not tell the complete story of just how much our law enforcement community relies on this technology each and every day. Numbers like these illustrate the value and importance of LPR technology to law enforcement."

About Vigilant Solutions:

Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:

Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Ohio Triple Homicide Suspect Located in New York using Commercial License Plate Reader Data

LIVERMORE, CALIFORNIA (September 3, 2015) – Vigilant Solutions announces today that Whitehall Police Department used its LEARN® investigative software and commercial license plate reader (LPR) data to locate a vehicle associated with a triple homicide on August 19th, resulting in an arrest of Daveron Minnis on August 25th by the New York City Police Department.

Sergeant John Grebbs explains, "The bodies of Kim Alston, Dontai Rheubottom, and Charles Fischer were found inside the Shaker Square Apartments on Olde Bailey Way near South Hamilton Road on Wednesday, August 19th. Through some investigation, it was determined that a white Dodge Charger was used as the getaway vehicle and Mr. Minnis was identified as one of the suspects."

"We entered the license plate of the Dodge Charger into LEARN in order to generate alerts should any vehicle in Vigilant's commercial LPR data network scan the plate. On Monday the 24th, we received an alert from LEARN that the suspect vehicle had been seen in Jamaica, New York, at 1:15 pm by an asset recovery vehicle using Vigilant's license plate reader equipment. Using the pictures provided, we confirmed that it was the correct vehicle. I immediately notified the NYPD and made them aware of the vehicle's location, but it was not there when they went to the scene." Vigilant copies the 100 million license plate scans made each month by asset recovery vehicles nationwide to its law enforcement data center in Virginia, making the data available to law enforcement for investigations and also for matching against various law enforcement hotlists.

Sergeant Grebbs continues, "On the very next day, August 25th, we received another alert that the license plate had been scanned again by one of these commercial vehicles at 11:43 am. It was in very close proximity to the scan from the prior day. I once again notified the NYPD with this information, and they were able to locate the vehicle in the area reported using a mobile license plate reader. Mr. Minnis was taken into custody and is being extradited back to Ohio where he will face three counts of homicide. The LPR data from Vigilant definitely assisted in this case, and saved countless hours and agency resources in locating our suspect."

About Vigilant Solutions:

Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:

Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Registered Sex Offender Identified and Apprehended Using Commercial License Plate Reader Data

LIVERMORE, CALIFORNIA (August 25, 2015) – Vigilant Solutions announces today that its LEARN analytic software and commercial license plate reader (LPR) data helped a Southern California law enforcement agency locate and apprehend a suspect in a sexual assault case against a mother and her two young daughters. Because of the nature of this case, the agency has requested to remain anonymous and have certain aspects of the case obscured.

One of the detectives on the case explains, "On July 4th, a mother and her two young daughters were exiting a grocery store, when a vehicle pulled in front of them and obstructed their path of travel. The driver of the vehicle leered at the young girls while holding an article of children's clothing and making an inappropriate sexual gesture. From the mother's account, we had a description of the suspect and his vehicle, but only had a partial license plate. We were unable to identify or locate the suspect and vehicle by conventional means or through other law enforcement databases."

"I ran a partial license plate search in the LEARN software, accessing over 80 million license plate detections in our immediate area, and almost 4 billion nationwide, and located one plate in our area that matched the vehicle description given by the mother. Using a different system, and with a permissible purpose authorized by the Driver's Privacy Protection Act, I ran a records check of the registered owner that revealed the vehicle belonged to a registered sex offender residing in the area. A search warrant was obtained for the suspect's residence and articles of children's clothing were discovered. The suspect was arrested without incident."

The detective concludes, "Basically we were able to identify this sexual predator in a matter of minutes using LEARN where conventional investigative and policing methods had failed. This could have taken much longer to accomplish the same result, possibly endangering many more potential victims."

About Vigilant Solutions:

Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:

Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Vigilant Solutions and Watch Systems team to deliver solution for improved registered sex offender compliance

LIVERMORE, CALIFORNIA (August 19, 2015) – Vigilant Solutions and Watch Systems announce today that they have worked together, and in close collaboration with mutual customers, to provide improved abilities to manage registered sex offender compliance efforts throughout the country.

Vigilant Solutions is the leading license plate recognition (LPR) technology provider in North America, and maintains the largest database of commercially-generated LPR data of over 3.5 billion detections. Watch Systems provides the nation's leading offender management and community notification solution managing over 60% of the nation's registered sex offenders and sending over 10 million notifications every year.

Working closely with Sacramento County Sheriff's Department who manages roughly 3,500 registered sex offenders, Vigilant Solutions integrated data from Watch Systems to deliver an automated hot-list capability that provides alerts on registered sex offenders' vehicles as they are seen by both law enforcement- and commercially-operated LPR systems. These alerts provide compliance officers insights into potential issues and discrepancies that may indicate non-compliance by the registered sex offender.

These alerts sometimes prompt subsequent investigations using Vigilant's LEARN® product which leverages Vigilant's national network of LPR data. Leveraging tools like Locate Analysis, a compliance officer can help validate or bring into question a registered sex offender's reported address(es). If an offender reports living at one address, but his/her vehicle is repeatedly seen over the course of a period of time in another City or State, this could indicate non-compliance and certainly provides the compliance officer with additional useful information. If a registered sex offender fails to report or is otherwise designated as an absconder, these same tools may be used to help locate and arrest these individuals.

Lou Luzynski, Co-Founder and Managing Partner of Watch Systems states, "When offenders realize they can't beat the system it engenders a notion that there is no use trying. And when offenders know they are being monitored, they find it much less tempting to repeat something they know they shouldn't do. Even more importantly, an offender that has gone stealth is often only a few steps away from another event; an event that every community wants to prevent."

Shawn Smith, President and Co-Founder of Vigilant Solutions adds, "The relationship with Watch Systems is one that typifies why we are here. "Protecting officers, families and communities" is our Company's passion statement, and these are more than just words to us. Every member of the Vigilant community makes a difference in the lives of so many – our employees, our partners, and most importantly – our customers. We are happy to enter into this relationship with Watch Systems as they also share in this belief."

About Vigilant Solutions:
Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Commercial license plate reader data helps locate suicidal missing person

LIVERMORE, CALIFORNIA (July 9, 2015) – Vigilant Solutions announces today that its LEARN analytic software and commercial license plate reader (LPR) data helped a law enforcement agency locate a suicidal missing person. Because of the nature of this case, the agency has requested to remain anonymous and have certain aspects of the case obscured.

A detective from the agency reports, "An officer from the Missing Persons Unit called me and requested that I run a missing person's license plate number through our LEARN database." LEARN accesses the LPR data that the agency's systems collect and also provides access to Vigilant's own network of over 3.5 billion commercially generated LPR detections. "The missing person's license plate had been scanned several times at a nearby address after she was reported missing, so officers were dispatched to the location. Upon arriving at the address, it was discovered that this was a parking lot for a retail store. The vehicle was located in the parking lot, and upon inspection a large blood stain was noticed in the driver's seat. There appeared to be more blood in the back seat."

"While waiting for the wrecker to tow the vehicle to the impound lot for further inspection, we went into the store and viewed video from the day the vehicle was first scanned at the location. We witnessed the vehicle entering the parking lot, and observed what appeared to be a female matching the description of the missing person exit the vehicle and enter the store. The subject entered the store and turned right in the direction of the restrooms. We continued to watch the video hoping to get a better view of the subject upon exiting the store. After approximately 40 minutes, we observed two uniformed officers entering the store and also observed several fire personnel enter the store only five minutes later."

"Upon further investigation, it was determined that emergency personnel responded to a call that night about a female who had attempted suicide in the women's restroom. The woman was taken to a nearby hospital and later transported to another hospital for further treatment. Because of this commercial LPR data, we were able to connect the dots in this investigation; the woman's identity was confirmed, her family was notified, and she was removed from the NCIC missing persons database."

Shawn Smith, Founder and President of Vigilant Solutions, comments, "We are thankful that these first responders were able to use our commercial LPR data and LEARN analytic tools to help locate this missing woman. In this case, we are pleased to find out that the woman was safe and already receiving medical attention, but we are hopeful that the ability to identify her aided in her treatment and recovery and brought some peace to her family."

About Vigilant Solutions:
Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Commercial license plate reader data helps apprehend suspect in multiple underage sexual assaults

LIVERMORE, CALIFORNIA (June 4, 2015) – Vigilant Solutions announces today that its LEARN analytic software and commercial license plate reader (LPR) data helped a law enforcement agency locate and apprehend a suspect in multiple sexual assaults against underage victims. Because of the nature of this case, the agency has requested to remain anonymous and have certain aspects of the case obscured.

One of the detectives on the case explains, "We had an individual identified as a suspect in multiple sexual assaults against several underage family members. When the investigation broke, the suspect fled the state in a vehicle that was not registered to him. We had a description of the vehicle, including the make, model, color, and other unique descriptors, but we had no license plate information.

"The suspect was believed to have fled to Mexico or was possibly staying with other family members in several states that border Mexico. Using LEARN's Stakeout feature, we remotely visited all the known family residences to see if there was any commercial LPR data that may assist in the investigation. We located a vehicle parked near one of the family member's residences that matched the description given to us by the victims. This image was shown to the victims who positively identified the vehicle as the one used by the suspect.

"With this positive visual confirmation, and with the full license plate number now available from the LPR detection, the vehicle was entered as a felony vehicle and the local police department was notified. The next day the local agency stopped the vehicle with the suspect inside. He was arrested and extradited, and he now faces twenty-five years to life as a sexual predator."

Brian Shockley, Vice President of Marketing for Vigilant Solutions, comments, "This is a great example of how commercially generated LPR data aids law enforcement. It goes without saying that, were it not for this data, this investigation would have taken much longer to resolve and would have consumed a far greater amount of resources from all of the participating agencies. Had this suspect not been arrested as quickly as he was, who knows how many more individuals may have been victimized? We applaud the agency for being vigilant in bringing this individual to justice, helping to bring closure to these young victims, and possibly preventing another horrible crime."

About Vigilant Solutions:

Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:

Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Commercial, Historical LPR Data Aids Texas Agency in Homicide Investigation

LIVERMORE, CALIFORNIA (May 7, 2015) – Vigilant Solutions announces today that its commercial license plate reader (LPR) data was used by a Texas law enforcement agency to help refute the alibis of suspects in a homicide investigation, resulting in an arrest. Because the case is still pending, the agency has requested to remain anonymous and have certain aspects of the case obscured.

The officer explains, "I received a call from our Detective in Homicide. He asked me if I would search a plate related to some potential suspects in a homicide investigation through the LPR database, which is not an uncommon occurrence. I grabbed my computer and searched the plate in LEARN."

"I called him back and gave him the most recent LPR detections for the vehicle and asked him if he would like any of the information emailed to him. He was especially interested in the detection for the day of the homicide, at approximately 0800. The Detective said the suspects claimed to be at their home in the south side of the City all day watching movies together. The LPR image of a vehicle they were known to drive was captured southbound on the interstate headed toward another town. I emailed the detection data to him, complete with color pictures of the vehicle. Armed with this new information, the Detective began questioning one of the suspects who – when confronted with the information – ultimately broke down and confessed to the shooting and admitted that they had left the City after the crime."

"This is a great example of the value of commercial and historical LPR data. Many times in a major crime investigation, it takes some amount of investigation – and time – to get to a list of potential suspects. As I know there is legislation around the country attempting to limit retention of historical LPR data, especially when the detection is not immediately related to a crime, we felt it important to get this story out there. This is a great example where this plate was not of interest to anyone when it was scanned, but only became of interest months later after other investigative work led us to these suspects. This one license plate detection in a database of over 3 billion saved countless man hours and also helped us make an arrest and take two dangerous individuals off the street – preventing future crimes, and perhaps even saving a life."

Tom Joyce, Vice President of Product Development for Vigilant Solutions and Retired Cold Case Commander for the New York City Police Department, comments, "With all of the conversation about LPR and privacy, it is important to note that this detection alone did not refute the alibi of the suspects. Why? Because LPR only identifies vehicles and has no way of determining who is driving a vehicle. The burden to place an individual in a vehicle still rests on the shoulders of law enforcement. LPR merely provides leads for these dedicated investigators and detectives to follow. We are thankful in this case that this lead was enough to help place these two dangerous individuals behind bars before they could perpetrate another crime and potentially bring harm to others."

About Vigilant Solutions:

Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:

Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Commercial License Plate Reader Data Aids Whitehall Police Department in Felony Assault Case

LIVERMORE, CALIFORNIA (April 30, 2015) – Vigilant Solutions announces today that the Whitehall Police Department in Ohio is using Vigilant Solutions' commercial LPR data, and it has resulted in a number of successes in only the first couple of months of use.

Sergeant John Grebb explains, "Detective Bureau Secretary Kellie McKinley and another Detective attended a meeting in Franklin County as they were in the process of deploying Vigilant Solutions. In this meeting, they learned of the commercial LPR data that is available from Vigilant, and the LEARN analytic tools to make use of this data as well as other data captured by law enforcement deployed LPR systems – whether they be from Vigilant or another vendor. As a result of the meeting, we began a trial of the LEARN system and the commercial LPR data."

"During the trial period, we had a notable success. Around 8 months prior to the trial of the Vigilant system, a vehicle was stolen and used in a felony assault in which a female was shot multiple times with an AK-47. The victim survived, however the injuries will impact the rest of her life. After obtaining access to the system, we began looking back at cases involving vehicles and noticed that there were multiple detections of the stolen vehicle used in this felony assault. Using this historical LPR data collected by commercial operators of LPR systems and made available through Vigilant's system, we were able to locate the vehicle. While the vehicle was unoccupied and had been abandoned for several months, the location of the vehicle proved to be a turning point in the case and provided significant evidence.

"This case really highlighted to our agency the importance of having this commercial data available for investigative use. While we have two LPR systems of our own, this historical, commercial license plate reader data is much more substantial than anything that we would have gathered using our own systems or by looking at LPR data gathered by other neighboring agencies with LPR systems. We used this case to highlight to our command staff how this data really becomes a force multiplier and effectively puts many more LPR systems to work for us, without the expense or administrative burden of acquiring and deploying our own network of LPR systems. The access to this data gave us insights that we would not have had otherwise, and saved us many man-hours of locating this vehicle and bringing justice to these individuals. It was shortly after this that we decided to move forward with Vigilant and we have already solved another case involving a stolen vehicle in only about a month of having the subscription."

Brian Shockley, Vice President of Marketing for Vigilant Solutions, comments, "We put an incredible amount of resources into helping educate legislators, the public, and our customers on how historical LPR data is anonymous in nature and how it may only be connected to registered owners – in another system – under permissible purposes defined and authorized by the Federal Driver's Privacy Protection Act (DPPA). This commercial LPR data can prove extremely valuable to law enforcement for investigations as Sergeant Grebb tells us in this case. Thanks to Whitehall for using all available resources to bring these individuals to justice and for helping to tell the real story about the value of historical, commercial LPR data. Stories like this are the best way to help people understand the good that this technology and data bring to society."

About Vigilant Solutions:

Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:

Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Historical LPR Data Aids Coral Springs in Locating Hit-and-Run Vehicle

LIVERMORE, CALIFORNIA (March 16, 2015) – Vigilant Solutions announces today that the Coral Springs Police Department used commercially generated and historical license plate reader (LPR) data, available through its LEARN® software, to locate an out-of-state vehicle with an expired registration that was involved in a hit-and-run collision.

Officer Rich Best of the Coral Springs Police Department explains, "We received a phone call from someone who had just observed a woman crash into his parked car. The woman stopped, and the two had a very brief conversation until he insisted on calling the police. She then quickly fled the scene and drove over a median in the process. I arrived on the scene approximately ten minutes after receiving the initial dispatch call. The victim was able to quickly snap a photo of the back of her vehicle with his cell phone. It was easy for me to see from the photo that the vehicle was a silver Audi A6 and had a Texas license plate attached. A records check determined the Texas tag was expired, assigned to a Honda, and registered out of New York to another individual. Based on this information, it was my belief that the investigation could possibly go unsolved due to a variety of issues and challenges the Traffic Investigator would face. Unfortunately and as a result, it was also likely that the victim and/or his insurance company would have to incur the loss.

I decided to give the LEARN database a shot. After logging in, I was pleasantly surprised to see the Texas license plate had been scanned on multiple occasions over the past four months in a nearby apartment complex. I verified the images and confirmed it was the same vehicle and same tag. Because of this data, we were able to locate the vehicle at the apartment complex within one hour of my arriving at the crash location. After speaking with neighbors in three different buildings, the investigation led to locating and identifying the driver of the vehicle, who was hiding in a rear bedroom of one of the apartments. The same driver ultimately ended up providing a confession to her actions and was subsequently arrested and charged with several crimes (leaving the scene of a crash resulting in property damage, utilizing a tag not assigned to her vehicle, driving with an expired driver's license, and not having any proof of insurance).

Additionally, the victim ended up positively identifying the person as the driver of the vehicle. We were fortunate to have some great resources at our disposal and were fortunate everything worked out in this case. The victim was completely shocked and could not believe in less than two hours after calling the Police Department, the hit and run vehicle was located and the driver was located, identified, and arrested. In fact, the victim stated, 'this is something you'd see on TV or in a movie'."

Officer Best went on to say "the Vigilant system and the data available are a tremendous resource and have proven to be helpful in solving crimes that could possibly go unsolved or take greater lengths and time to solve. Like our Detectives who used the systems a couple of years ago to locate a missing woman who was near death, I am a firm believer in the power of the system. It solves crimes and saves lives."

About Vigilant Solutions:
Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Hillsboro Police Arrest Fugitive Using License Plate Reader (LPR) from Vigilant Solutions

LIVERMORE, CALIFORNIA (January 29, 2015) – Vigilant Solutions announces today that the Hillsboro Police Department in Oregon used a Vigilant Solutions License Plate Reader (LPR) system to locate and apprehend a fugitive with multiple warrants.

Lieutenant Michael Rouches comments, "Hillsboro police officers were patrolling the Fred Meyer parking lot utilizing the License Plate Reader (LPR) system to check license plates as they drove through the parking lot. The system works by reading the characters on license plates to see if they match license plates in law enforcement databases. It is important to note that the system does not collect, or even have the ability to access, any personal information such as the name of the owner – it works anonymously and tells us if the numbers and letters that it sees on the plate match the numbers and letters in a database. In addition to the federal law that protects driver's privacy, we also have a strong policy that defines the permissible uses of the system as well as training requirements."

"The LPR system alerted officers to stolen license plates on a 2014 stolen Kia Sorrento SUV. The plates were stolen from Portland Oregon and the vehicle was reported stolen out of King County Washington. It is not uncommon for individuals to change the license plates on vehicles that they steal in efforts to avoid detection – and, stolen vehicles are often precursors to other more serious crimes. Without the LPR system, it would have been very unlikely for an officer to identify that this vehicle were stolen if the vehicle were driving lawfully or simply parked in a parking lot."

"Officers waited for the driver of the vehicle who returned a short time later. Officers contacted the vehicle driver and he was confirmed to be a wanted fugitive out of Washington State with warrants for Robbery, Felon in Possession of a Firearm, Possession of a stolen vehicle and Contempt of Court. The fugitive was placed under arrest on these warrants and the stolen vehicle charge from this case, which remains pending."

Scott Dye, retired Police Lieutenant and Regional Manager for Vigilant, comments, "It is great to see Hillsboro having success with their system. LPR truly is a game changer for law enforcement, helping them identify vehicles that they normally would've driven right by, improving officer safety by letting them know of potentially dangerous situations before they occur, and helping develop investigative leads through the use of the collected, anonymous, data."

About Vigilant Solutions:

Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:

Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Armed Robberies Dating Back One Year Solved Using Vigilant License Plate Reader (LPR) and Historical LPR Data

LIVERMORE, CALIFORNIA (January 13, 2015) – Vigilant Solutions announces today that Conyers Police Department used its license plate reader (LPR) system, historical LPR data and LEARN® analytic software to identify and apprehend a suspect in a series of at least thirty-five armed robberies dating back over one year in Conyers, Georgia and other areas around the state.

Sergeant Guy Sanders explains, "A masked man armed with a handgun robbed a local title loan and pawn shop, Title Bucks, here in Conyers. The suspect locked the employees and a customer in the back room before he fled the scene. Prior to receiving the 911 call, Officer Spencer Holland noticed a two-toned black and tan Ford Expedition driving erratically in the area. The officer was on his way to another call, so he was unable to address the violation at that time. A short time later, Officer Holland saw the Expedition again heading away from the Title Bucks location. Officer Holland's patrol unit is equipped with a Vigilant License Plate Reader (LPR) system which captured and recorded the Expedition's tag information as he responded to the robbery call that had now been dispatched.

Officer Holland recalled a previous lookout for a black over tan SUV involved in a similar title pawn robbery in Gwinnett. Only two days later, the same Ford Expedition was again captured on camera leaving the area of another title pawn robbery in Newnan, Georgia. As a result, having proper cause under the Driver's Privacy Protection Act (DPPA), the vehicle license plate was used to look up the registered owner for the vehicle, and an arrest warrant was issued for the suspect for Armed Robbery, Kidnapping, and Aggravated Assault. With the assistance of the FBI, the suspect was located and taken into custody without incident. The ongoing investigation now has the individual in custody suspected of at least thirty-five similar robberies through the state dating back well over a year. The LPR system from Vigilant and the historical data in LEARN was the catalyst that broke the investigation wide open."

"We are happy to hear that Conyers has seen success with the system, and we are confident that they will see many more successes in the future," states Brian Shockley, Vice President of Marketing. "This technology and the historical data have a remarkable ability to help develop leads in pattern crimes and major crimes investigations. Congratulations to the Conyers PD on a job well done."

About Vigilant Solutions:

Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:

Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Homicide Suspect Located using Historical License Plate Reader Data

LIVERMORE, CALIFORNIA (October 16, 2014) – Vigilant Solutions announces today that the Sacramento Police Department used its historical license plate reader (LPR) data, available exclusively to law enforcement through Vigilant's LEARN® online analytic suite, to locate and apprehend a suspect in a homicide.

Sergeant Stigerts of Sacramento Police Department explains, "A homicide occurred in City of Sacramento on April 23rd of this year. A follow up investigation conducted by detectives identified the shooter as well as a vehicle registered to him and to his mother which matched the description of the get-away vehicle. Investigators also determined that the suspect was believed to live with his mother in Sacramento and was attending a junior college in Rocklin. Detectives initially checked for the suspect vehicle in various locations in the immediate Sacramento area where the suspect was known to stay with negative results. Detectives checked the LEARN database for any information available on the target vehicle as well as to verify the unique appearance of the vehicle as relayed by witnesses."

"In this case, detectives were able to put the suspect plate number into LEARN and quickly realized that it appeared in Vigilant's private data multiple times in a specific apartment complex near the college where the suspect attended classes. They were also able to confirm the appearance of the suspect vehicle through recent LPR snapshots of the car. We were able to send Rocklin Police this information and have them determine if the suspect vehicle was on scene. We knew within a matter of a few phone calls that the target vehicle was indeed in the apartment complex in Rocklin, located in neighboring Placer County. Surveillance was quickly set up by Sacramento and Rocklin police officers on the location; and in the morning after the homicide, the unaware and unarmed suspect walked out of the apartment, was identified by police and safely detained without incident."

The Sergeant concludes, "The murder weapon was later located inside the apartment shortly thereafter and the situation was resolved without high cost or a lengthy stand-off. Through simple coordination with the neighboring jurisdiction we were able to take a homicide suspect into custody within a few hours, rather than a few days as is our typical course without private LPR data."

Tom Joyce, Vice President of Product Development for Vigilant, comments, "This is a great example of how LPR data can and should be used. Governed by a strong agency policy as well as federal law, the anonymous LPR data provided an investigative lead that brought a dangerous individual into custody. Having worked thousands of cases during my career at the New York City Police Department, I can't tell you enough how valuable this type of information can be in saving an immense amount of taxpayer funded resources – as well as potentially saving lives in the process by taking these dangerous individuals off the streets before they commit further crimes."

About Vigilant Solutions:
Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Over 100 Florida Law Enforcement Agencies Rely on Vigilant Solutions

LIVERMORE, CALIFORNIA (October 8, 2014) – With just over two weeks remaining until the International Association of Chiefs of Police (IACP) Annual Conference and Exposition in Orlando, Vigilant Solutions reports today that over one hundred (100) law enforcement agencies in Florida are relying on Vigilant Solutions' license plate reader (LPR) data, analytics and hardware solutions.

Brian Shockley, Vice President of Marketing, states, "Over 100 agencies in the state have joined over 3,000 nationwide in using Vigilant for their LPR needs. In just the past year, agencies in Florida have used Vigilant in the investigation of literally thousands of investigations. One relatively high-profile example shared with us out of Hollywood, Florida, involves the Economic Crimes Unit leveraging the power of Vigilant's LPR data network to locate a couple that had defrauded an elderly victim of about $300,000. The suspects were located in Las Vegas, taken into custody by Las Vegas Metro Police Department, and extradited back to Florida. This is just one of many examples we have where our data and LEARN® analytic software have proven successful even before an agency has deployed its first LPR system."

"To support our continued growth within the state and also to comply with FDLE's desire to have all LPR hotlist data housed inside the state, Vigilant has invested the needed resources and acquired a server network to satisfy the needs of the state. Much like our secure law enforcement data center in Virginia which currently manages over 2.5 billion detections and tens of thousands of law enforcement users from around the country, the Florida server provides a scalable LPR solution in the cloud to any agencies that want to take advantage. This LEARN server is housed at Miami Beach Police Department and managed by Vigilant. This LEARN server is able to integrate any and all competitive hardware, as we are currently doing for many agencies around the country, to provide more powerful analytics, simplified data sharing, and supplemental LPR data not available anywhere else."

Tom Joyce, Vice President of Product Development, adds, "Leveraging the strength of our engineering team of more than seventy individuals, there are many exciting developments underway – some near term, some longer term. New analytic tools, new sets of data to enhance both our LPR and facial recognition offerings, and our new Mobile Companion app for smart phones and tablets are just a few of the items that our customers will be hearing about very soon. And, as always, new features and tools are automatically deployed and available in the cloud at no extra cost. We are excited about our future, and what we can do for our customers."

About Vigilant Solutions:
Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

High Volume Drug Traffickers Apprehended Using Historical License Plate Reader Data

LIVERMORE, CALIFORNIA (August 21, 2014) – Vigilant Solutions announces today that the Maryland State Police credit Vigilant's own network of private and historical license plate reader (LPR) data and online investigative tools in the location and apprehension of four individuals trafficking large volumes of cocaine and marijuana between the desert southwest and various locations on the east coast.

Sergeant Mujaihid Jones, explains, "One of the suspects was working with three co-conspirators to distribute large, multi-thousand pound, quantities of drugs including cocaine and marijuana. This suspect relocated to the desert southwest in 2012 where he worked with his conspirators, who provided him housing and paid for his services, to package and ship large quantities of drugs to various cities on the east coast. All four have been arrested, entered guilty pleas, and received prison sentences ranging from 10-14 years each on charges related to drug possession and distribution as well as money laundering."

"Without revealing specifics in our investigative methods, as this may jeopardize other investigations, I can say that the historical data available from Vigilant Solutions network of privately collected LPR detections was very helpful in the investigation and gave us supplemental data to that obtained from our own LPR systems," comments Sergeant Jones. "Search warrants executed as part of the investigation resulted in the discovery of large sums of cash and cash bank deposits, almost half a million dollars in jewelry, firearms and assorted body armor, as well as various quantities of marijuana and cocaine. Additionally, as part of the plea agreements entered, these items as well as interests in multiple properties, vehicles, and other goods were forfeited."

Sergeant Jones concludes, "We greatly value the capabilities enabled by Vigilant Solutions through their LPR data and online tools. This is one of several high-profile cases in which the data has assisted our agency in taking dangerous individuals off the street, including the case of Edgar Daniel Mazariegos-Cifuentes who abducted a fifteen year-old girl in 2012 whom we located and rescued based on LPR data."

Shawn Smith, Founder and President of Vigilant Solutions comments, "We are always pleased to hear stories like this of bad guys being taken off the streets – resulting in safer communities for us all. While we are glad to hear that our data and tools played a role in this case, we should never forget that the ultimate credit goes to the many men and women in uniform. Without their dedication, insight, and vigilance, we would all live in a very different world."

About Vigilant Solutions:
Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Violent Gang Member Suspected of Killing 14-Year-Old Boy Apprehended Using Vigilant Solutions' License Plate Reader Data

LIVERMORE, CALIFORNIA (July 22, 2014) – Vigilant Solutions announces today that the use of its License Plate Recognition (LPR) data and LEARN® online investigative solution has resulted in the successful resolution of a gang investigation. The details of the case are being obscured at the request of the agency.

The agency belongs to one of the largest multi-jurisdictional LPR initiatives in North America. The initiative comprises multiple agencies serving a population of over 3 million. One of the investigators on the case states, "Our agencies selected Vigilant for many reasons – the performance and accuracy we observed during our evaluation, the flexible architecture, the ability to integrate our existing LPR hardware from another vendor, cloud-based data sharing, good analytic tools, and other reasons. One really unique element of the Vigilant system that has proven valuable is the private data network, which recently helped us put some dangerous gang members behind bars."

"A member of one gang stabbed a member of a rival gang sparking a series of incidents," reports the investigator. "In retaliation for the stabbing, the rival gang conducted a 'drive-by shooting' at a known location of the other gang, hitting and killing a 14-year-old boy." The investigator immediately turned to Vigilant for leads on the suspect's whereabouts.

Searching the almost 2 million LPR reads collected monthly by the nearby agencies, and supplemented by over 4 million additional reads collected by the Vigilant private data network, detectives were able to identify several sightings of the suspect's vehicle in the area. The investigator continues, "Many of these were at a nearby strip mall. Without additional information, this would have been extremely useful to our team as it is likely a workplace of the suspect, but as it turned out that we didn't need this information. We had a sighting of the suspect license plate parked at a residential location within minutes of the incident. I almost fell out of my chair."

"We deployed an apprehension team immediately where the suspect and a friend were seen leaving the residence and getting into their vehicle. The apprehension team followed the suspect to a nearby location and took them safely into custody without incident. This single LPR detection provided by Vigilant greatly expedited our investigation, potentially saved hundreds of man-hours, and allowed us to get this dangerous suspect off the streets quickly before the situation escalated further and another incident occurred."

About Vigilant Solutions:
Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Serial Rape Investigation Brought to Closure Using 4-Year-Old License Plate Reader Data

LIVERMORE, CALIFORNIA (June 4, 2014) – Vigilant Solutions announces today that its commercial license plate reader (LPR) data provided an investigative lead into a serial rape cold case dating back over four years. The details of the case have been obscured at the request of the agency and due to the ongoing legal process.

The Detective sharing the story states, "Our department received an anonymous tip in a serial rape investigation. The series of rapes occurred over several years and in multiple counties. All the rapes were believed to have been perpetrated by the same individual. Security video had captured the suspect and his vehicle at the location of one of the rapes that occurred four years prior to the tip. However, the security video did not provide a vehicle color or license plate. DNA and fingerprint evidence did not provide any matches indicating that the serial rapist did not have a criminal record. The case was cold until the anonymous tip was called in."

"The anonymous tip provided a possible suspect name," continues the Detective. "Since the vehicle license plate was not visible in the security tape I was asked to examine the video. While watching the video I noted several distinct characteristics that appeared on the vehicle in the security video. Having a legitimate investigative purpose, I requested and received a DMV report listing the vehicles that had been registered to the suspect during the time and dates of the rapes. The DMV report listed a vehicle matching the make and model seen in the video.

With this new information, I ran a query in Vigilant Solutions' LEARN software against its national LPR database consisting of data that Vigilant collects through its commercial operation, and also of data collected and shared by law enforcement agencies. I located multiple historical scans that showed not only the vehicle color, but also the same distinctive characteristics that appeared in the security video. At this point, we knew we had found our man. Because of the number of historical scans available, we were able to document the vehicle's appearance and condition prior to the date of the incident, during the time of the incident, and after the date of the incident."

The Detective concludes, "The data and images provided by the Vigilant system (4 years after the date of this particular rape) were instrumental in helping to make the case against this suspect and take a dangerous predator off of the streets. It should be noted that until this anonymous tip, these LPR scans were never the subject of inquiry…only anonymous bits of data that had to be connected to an individual in the course of an active investigation."

Brian Shockley, Vice President of Marketing for Vigilant Solutions, comments, "This is a perfect example of how LPR data, commercially gathered and well-aged, can be extremely valuable in a major crimes investigation. We are delighted that this information was available to assist in this case, and wasn't legislated away by an arbitrary retention policy."

About Vigilant Solutions:
Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Alabama Criminal Justice Information Center Leverages License Plate Recognition Analytics and Data from Vigilant Solutions

LIVERMORE, CALIFORNIA (April 24, 2014) – Vigilant Solutions announces today that the Alabama Criminal Justice Information Center (ACJIC) has implemented Vigilant Solutions for its hosted license plate recognition (LPR) analytics and LPR data.

ACJIC purchased seven (7) mobile license plate recognition systems from Vigilant Solutions for statewide enforcement efforts. The seven systems have been deployed around the state and are managed by an ACJIC account on Vigilant Solutions' hosted law enforcement data center. The use of the Vigilant data center allows for the data to be easily accessed by authorized users from any web browser, and also eliminates the need for investment in server hardware while ensuring scalability and data security.

Vigilant Solutions' cloud data center also provides a simplified approach to LPR data sharing. Alabama agencies using Vigilant Solutions, such as the Jefferson County Sheriff's Office, Hoover Police Department, Bessemer Police Department, Auburn Police Department, and others, have the ability to automatically share their LPR data to the ACJIC for statewide investigative efforts. In addition to Alabama agencies, other Vigilant agencies nationwide, such as Dallas and Atlanta which share the I-20 corridor, may also choose to share with ACJIC. Agencies using competitive LPR systems may be integrated into the Vigilant data center to take advantage of Vigilant's secure and scalable cloud-based solution.

Vigilant's LEARN® software, which also resides on the Vigilant law enforcement data center, provides powerful querying along with exclusive analytic tools to generate investigative leads and insights and ultimately bring cases to closure more quickly.

"Vigilant is proud to add the ACJIC to its list of satisfied customers, and we look forward to their insights into how we can continue to build out our product capabilities to assist our law enforcement customers in their very important jobs of protecting our families and communities," states Tom Joyce, Vice President of Product Development and retired Lieutenant/Commander of the New York City Police Department.

About Vigilant Solutions:
Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Bexar County Constable Improves Safety of San Antonio Stock Show and Rodeo with License Plate Recognition from Vigilant

LIVERMORE, CALIFORNIA (MARCH 25, 2014) – Vigilant Solutions announces today that the Bexar County Constable's Office, Precinct 3, used its license plate reader (LPR) system at the San Antonio Stock Show and Rodeo to improve its enforcement of local warrants and also make a number of arrests, improving the safety for those attending the event.

Bexar County Constable Mark Vojvodich, states, "The San Antonio Stock Show & Rodeo attracts nearly one and a half million visitors. With this many people converging into a relatively small area, it provides a great opportunity to go and peacefully enforce some of the outstanding warrants in our County. Many of these warrants are a result of people failing to pay a simple traffic citation or failing to appear in court. The original fines were issued to discourage unsafe driving habits – habits that are proven to endanger lives and property. If we fail to enforce these fines, then there are no consequences for those committing offenses and the unsafe behavior continues. If we are able to consistently enforce these fines, then over time we hope to see a reduction in citations due to voluntary compliance of our laws. All of this results in safer roadways and lives saved."

"The warrant roundup effort was extremely successful," adds Vojvodich, "as we cleared 142 warrants and made 41 arrests in roughly one week. The LPR system from Vigilant, using a hotlist we created from our outstanding warrants, was used to scan the parking lots and streets surrounding the event helping us to locate these individuals. We were able to peacefully resolve and clear 142 warrants which is good for both the County and the individuals involved. We were able to avoid arrests and prison time for many of these individuals, and almost $30,000 in outstanding funds due to the County were collected. Many do not realize that these funds can offset property taxes, help fund better schools, and improve infrastructure. This effort would not have been possible without the LPR technology from Vigilant."

Founder and President of Vigilant Solutions, Shawn Smith, states, "Bexar County Constable Vojvodich is a real leader that cares about his community. We applaud him for his efforts to make a difference in Bexar County, and look forward to continuing our great relationship."

About Vigilant Solutions:
Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

License Plate Reader Data Enables Police Department in Connecticut to Apprehend Suspects in Purse Snatch and Assault of Pregnant Woman

LIVERMORE, CALIFORNIA (March 3, 2014) – Vigilant Solutions announces today that the Fairfield Police Department in Connecticut used its license plate reader (LPR) data and LEARN software to solve a purse snatch case involving an assault on a pregnant woman.

Deputy Chief Chris Lyddy reports on the case, "On February 21st, we had a very bad purse snatch. A young woman, 6 months pregnant, was walking out of a local gas station when a suspect wearing a hoodie grabbed her purse. The suspect jumped into a dark color Nissan. The pregnant woman, in trying to retrieve her purse, was dragged by the suspect's vehicle as he attempted to flee. The woman had to be hospitalized due to her injuries."

"We thought that we had caught a break when a witness reported a license plate for the suspect vehicle," continues Lyddy, "but in running the plate against Connecticut DMV data there was no match. Surveillance video from the store was obtained, but it was poor quality and also yielded nothing for us other than to confirm the vehicle description. Knowing that witnesses sometimes do not accurately recall license plate numbers, and having just received access to Vigilant's online LEARN software and national LPR database, I decided to try searching various partial plate combinations. We developed a list of around 750 possible suspect vehicles, but these were all eliminated through the course of the night."

Lyddy continues, "The next morning, I returned to the office and continued searching the database as new LPR data is always coming in from Vigilant's network. I searched every few hours, until finally at 3pm that afternoon, I found a match on a partial plate that looked like the suspect vehicle and was in relatively close proximity to the crime scene. With this new lead, and marrying the full license plate number to an individual through DMV records, we were able to quickly have some officers go and monitor the vehicle at the location."

"One hour later, a male wearing a hoody and a female entered the vehicle and left the location. Officers stopped the vehicle, and within only a few minutes, both confessed to the purse snatching, the purse was recovered, and the two suspects were arrested. Most importantly, the mother and baby are doing well and are expected to fully recover."

Lyddy concludes, "I am thankful for the availability of this data collected by Vigilant and made available to law enforcement, as we may not have solved this crime otherwise. I hope that the legislators that are looking to abolish the commercial use of LPR in Connecticut think about the impact that this will have on public safety. My budget simply would not allow for the same level of service that Vigilant can provide through its operations."

About Vigilant Solutions:
Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Child Molestation, Armed Robbery and Car Jacking Suspects Arrested with Assistance of License Plate Readers

LIVERMORE, CALIFORNIA (February 3, 2014) – Vigilant Solutions announces today that the Loganville Police Department in Georgia attributes recent and significant arrests to their use of license plate recognition (LPR) technology from Vigilant Solutions.

Assistant Chief M.D. Lowry comments, "On January 7, one of our officers received an alert from his license plate reader (LPR) system on a vehicle which was associated with an active arrest warrant out of Texas. Our officer initiated a traffic stop per policy and identified the driver. Following protocol, the officer used other systems to validate the hit and was able to confirm the driver was wanted out of Del Rio, Texas for Indecent Acts with a Child, 2nd Degree. The suspect was taken into custody without incident and transported to the Walton County Jail to await extradition. "

"Just shortly after processing this suspect and within less than two hours of the first hit," continues Lowry, "the officer returned to patrol and received another alert from his LPR system on a stolen vehicle out of Doraville. The officer attempted to stop the vehicle, however the driver accelerated and a short pursuit ensued. The driver of the suspect vehicle lost control in a turn because of their high speed and the vehicle ending up in the wood line adjacent to the roadway. The female driver jumped out of the vehicle while it was still moving and ran into the woods. To protect other drivers on the roadway, the officer first focused on stopping the moving vehicle before it veered into oncoming traffic, and then requested additional units to set up a perimeter around the area. Units from the Loganville Police Department and Walton County Sheriff's Office responded and set the perimeter while a K-9 unit was en route. Due to the extreme cold that night, the suspect surrendered to officers on scene. Follow-up investigation on this stolen vehicle determined it was taken in an armed robbery and carjacking in the city of Brookhaven. The suspect taken into custody was later identified by photographic line-up as having taken part in the robbery."

Assistant Chief Lowry concludes, "These two arrests took place in less than two hours by one officer equipped with LPR. I have no doubt that these vehicles would have passed through our jurisdiction without detection had we not had the LPR unit in place. We have only had our single unit for only a few months, but it is already proving its value by helping us to remove these threats from our community. I can tell you that the capture of a child molester from nearly 1,200 miles away was more than worth the cost of the LPR unit. If we never make another case with it, it was worth the cost."

About Vigilant Solutions:
Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Drive-by Shooting Solved with Assistance from Historical License Plate Reader Data

LIVERMORE, CALIFORNIA (January 28, 2013) – Vigilant Solutions announces today that Travis County Sheriff's Office used Vigilant Solutions' LEARN software, enhanced with additional license plate recognition (LPR) data from Vigilant, to assist in the identification and location of a vehicle used in a drive-by shooting.

Detective Alan Howard of Travis County Major Crimes Unit, who responded to the scene, explains, "I reported to the scene of the shooting, and through interviews determined that a young man was visiting his girlfriend at her home. A vehicle pulled up to the residence, and another young man exited the vehicle. The two young men got into a confrontation, but the suspect returned to his vehicle and the vehicle left the scene. A short time later, the vehicle drove by the residence, shots were fired from the vehicle, and the boyfriend and a bystander were injured. A witness to the shooting captured some video using a cell phone, and from that we were able to get a partial license plate and vehicle description. I sent this information to Detective Mark Wester for assistance in identifying the vehicle."

"I received the information from Detective Howard and decided to run the partial plate against historical LPR data that we had just gotten access to from Vigilant Solutions," adds Detective Mark Wester. "I logged into our agency's LEARN account, entered the partial license plate number, and received numerous matches to the partial license plate. One of these vehicles matched the description given to us by the witnesses, so we used this license plate to continue our investigation in hopes of identifying potential suspects. Using the full license plate number, and looking at Vigilant's historical LPR data dating back several years, we were able to determine a probable location for the suspect vehicle."

Detective Howard concludes, "Using the information that Detective Wester was able to pull from the Vigilant system, we were able to locate the suspect vehicle. This, in combination with other information, has allowed us to make four arrests in connection with the shooting. We are thankful that this historical data was available to assist us in this investigation."

"We applaud Travis County, one of our newest customers, for their use of our technology and our data to help identify and locate these suspects," states Shawn Smith, President and Founder of Vigilant Solutions. "With legislation pending in roughly half of the States to limit the amount of time that this historical LPR data may be retained, we are hopeful that stories like this will illustrate that this information is enabling law enforcement to more efficiently conduct major crimes investigations – protecting us all, preventing crime, and saving lives."

About Vigilant Solutions:
Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Fayette County Sheriff Uses Historical LPR to Nab "Pillowcase Bandit"

LIVERMORE, CALIFORNIA (December 18, 2013) – Vigilant Solutions announces today that its license plate recognition (LPR) systems, LPR data, online investigative tools and data sharing assisted the Fayette County Sheriff's Office in locating and apprehending the "Pillowcase Bandit."

Lieutenant Ethon Harper explains, "We were seeing a significant increase in residential burglaries in Fayette County leading into the holiday season. All of the burglaries featured a similar modus operandi (MO) as the burglar would use one of the homeowner's pillowcases to carry the stolen items from the home. Because of this, we named him the 'Pillowcase Bandit'."

"We received a lead from a homeowner on a suspicious vehicle – a gold colored Chevy – and we were able to couple this with information from other eyewitnesses, video surveillance, and historical LPR data to develop a potential suspect. During the course of the investigation, we shared this information with other neighboring counties including Coweta, Henry, Clayton, and Cobb and discovered that they too had experienced similar crimes. Running our suspect's license plate through Vigilant's LEARN software, which accesses other agency's shared LPR data along with that provided from Vigilant, we were able to place the vehicle in the vicinity of some of the other burglaries," continues Harper.

Harper adds, "Because a license plate is not a person, this was not enough information to make the case. The burden of placing our suspect with the vehicle was still on our shoulders, and we were able to do this through other investigative means. Our suspect was arrested and charged with multiple counts of burglary. The arrest led to the recovery of some of the stolen property including a firearm. We were able to identify the 'fence' for the stolen jewelry and arrest him as well."

Concluding, Lieutenant Harper says, "This is a great example of how sharing LPR systems and historical data can assist investigations. We began using LPR roughly four years ago, and after switching to Vigilant this year, we are seeing some great results from our seven mobile systems and the online tools they provide."

Shawn Smith, Founder and President of Vigilant comments, "Cases like this demonstrate the importance of community involvement. Were it not for that lead given by the concerned homeowner, the 'Pillowcase Bandit' may still be out there. It is also a testament to the good police work of the Fayette County Sheriff's Office – coordinating with other nearby agencies and using many different resources to accomplish their goal."

About Vigilant Solutions:
Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Bank Robber Apprehended Using Fixed License Plate Recognition Cameras from Vigilant Solutions

LIVERMORE, CALIFORNIA (November 25, 2013) – Vigilant Solutions announces today that its fixed license plate recognition (LPR) cameras were credited in the apprehension of a man wanted for a recent bank robbery in Great Neck, New York.

Commissioner John "Jack" Miller explains, "A Chase bank branch in Great Neck was robbed on September 27th, and a woman witnessing the robbery provided information on the subject involved. Using video surveillance from nearby businesses, we were able to locate a vehicle and subject matching the woman's description. This information coupled with our Village Camera system yielded a license plate number. The license plate number was then entered into our license plate recognition system to provide notification to the department when the vehicle was seen by one of our fixed LPR cameras, provided by Vigilant Solutions. We implemented our LPR program almost five (5) years ago, and it will soon consist of around fifty (50) fixed cameras, along with several mobile systems."

"Roughly one week later," continues Commissioner Miller, "the vehicle passed one of the fixed LPR cameras, generating an alert that the suspect vehicle had entered the village. We notified other area police departments on the peninsula who helped to locate the vehicle. Within about 45 minutes we had the suspect in custody, and he was charged with first degree robbery and first degree use of a criminal firearm."

Commissioner Miller concludes, "The system will soon cover all entrances to our village. While it is typically used to identify uninsured and stolen vehicles, this is a great example that demonstrates how the system assisted in a major crime and helped us apprehend an individual that presented a threat to our peaceful community. It's also important to note that the system is not used for red light violations or revenue generation of any type – it exists solely to protect our officers and our citizens by allowing us to be more efficient in locating vehicles associated with criminal activity. Clearly, it is working."

About Vigilant Solutions:
Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Hollywood Police Department Locates Interstate Fugitives with Vigilant Solutions

LIVERMORE, CALIFORNIA (November 14, 2013) – Vigilant Solutions announces today that the Hollywood Police Department in Florida used Vigilant Solutions to bring two interstate fugitives to justice.

Detective Daniel Justus explains, "As part of the Economic Crimes Unit, I was assigned a case involving an elderly victim of 89 years of age. Over the course of three months, he was scammed for a loss approaching $300,000. Through investigative work, I was able to identify two suspects, a female and her husband. I confronted these two suspects and provide them an opportunity to give a statement prior to filing a warrant for grand theft and elderly exploitation."

"The next day, realizing their predicament, they disappeared. We had no idea where they had fled, and we looked for approximately two months using conventional methods with no success. Having been in contact with Vigilant Solutions to discuss their license plate recognition (LPR) systems and facial recognition, I was aware of their national LPR data network which has LPR scans from all over the country in excess of 1 billion detections. Having no other viable leads, I contacted them and asked if they had any information on my suspect's license plate, " continues Justus. "I was pleased when they provided me with temporary access to the LEARN software which showed multiple sightings of the vehicle roughly 2,500 miles away in Las Vegas."

Justus concludes, "I made contact with the fugitive squad of Las Vegas Metro PD, and both suspects were taken into custody without incident on 1st and 2nd Degree felony charges. The suspects are awaiting extradition at present thanks to Vigilant's LPR data network and LEARN software. This arrest would not have been possible without the information from Vigilant, and these suspects would have likely disappeared with the $300,000 taken from our elderly victim. I believe in the investigative potential for Vigilant's solution, and I hope to get this great tool for our department."

Shawn Smith, Founder and President of Vigilant Solutions, states, "I'm extremely pleased to hear of this level of cooperation between one of our sales managers and the Hollywood PD. This is a great example of one of our team members thinking less about making a sale and more about our passion to protect officers, families and communities. We applaud Detective Justus for being vigilant in his responsibilities, and for not giving up in his desire to apprehend these suspects and bring closure to the victim."

About Vigilant Solutions:
Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Sacramento County Sheriff's Department conducts Operation Trick or Treat on Area Criminals with Vigilant Solutions License Plate Recognition

LIVERMORE, CALIFORNIA (NOVEMBER 1, 2013) – Vigilant Solutions announces today that the Sacramento County Sheriff's Department and other area agencies conducted a one-day sweep of Sacramento County using its license plate recognition (LPR) systems and historical LPR data to yield impressive results.

Operation Trick or Treat was conducted on Wednesday, October 30th, to demonstrate the effectiveness of license plate recognition systems installed on patrol cars and to highlight the use of how historical data is useful not only for investigations, but also in coordinated patrol operations. Sergeant Kyle Hoertsch comments on the results, "The operation far surpassed my expectations. We scanned around 70,000 license plates which yielded over 400 vehicles of interest in only six hours. Over 25 recovered stolen vehicles and around the same number of arrests were made. The arrests included a number from occupied stolen vehicles, but the majority were made possible through the use of historical LPR data from Vigilant Solutions as well as our own agency data to locate individuals with outstanding warrants, including many DUI's. In addition to these results, we also located a missing person vehicle, a stolen tractor trailer out of Tennessee, and we reunited two owners with their stolen cars."

The operation was a coordinated effort among several agencies, coordinated by Sergeant Hoertsch. "It was the historical data that was very helpful to us in locating individuals with outstanding warrants. Many of these individuals are difficult to locate, and the historical LPR data allowed for us to identify probable locations for these wanted individuals. I can say that Sacramento County is a safer place as a result of our operation."

The owner of one of the stolen vehicles that was recovered and returned commented that she was very grateful for Sacramento County Sheriff's efforts and for the technology that allowed her car to be returned to her. When asked if she minded having her license plate scanned, she said, "By all means, please do."

Founder and President of Vigilant Solutions, Shawn Smith, was present for the operation and states, "It was impressive to see our technology in action, and we applaud Sergeant Hoertsch for taking the initiative to coordinate this sweep and send a message to the criminals within Sacramento County that if they commit a crime, they will be caught. The criminal elements in Sacramento County will not enjoy the safe haven they may have in other locations where LPR data is quickly deleted and where the use of commercial LPR data for law enforcement purposes is prohibited."

About Vigilant Solutions:
Based in Livermore, California, Vigilant Solutions is an industry-leading pioneer of innovative intelligence solutions that help law enforcement protect officers, families and communities. For additional information, visit www.vigilantsolutions.com.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Cobb County Police Department Solves Homicide Using License Plate Recognition Data

LIVERMORE, CALIFORNIA (October 1, 2013) – Vigilant Solutions announces today the Cobb County Police Department in Georgia used Vigilant Solutions license plate reader (LPR) systems and data to identify two suspects in the homicide of a missing person.

Sergeant Larry "Ski" Szeniawski of the Cobb County's Homicide Unit explains, "We had a missing person report submitted with the agency, and the person had been missing for three days prior to the family making the report. I put out a flyer on the individual, in hopes of locating him. The flyer included the victim's vehicle description and license plate number. Detective David Thorp received the flyer and ran the license plate through the Vigilant Solutions LPR database to see if the license plate had been captured by any LPR devices contributing to the Vigilant's national LPR data sharing initiative."

"Upon querying the plate, we did find a sighting of the vehicle outside of town and after the person went missing. We went to the location, and the vehicle was no longer there, but this piece of evidence prompted us to retrieve video footage from the store's security cameras for the time that we knew the vehicle was in the parking lot. A review of the video footage revealed two acquaintances of the missing person at the store with the missing person's vehicle. This was a major breakthrough in the case that would not have been possible without the historical LPR data – the historical LPR detection told us exactly where to find the needle in a very large haystack," continues Sergeant Szeniawski.

Sergeant Szeniawski concludes, "We turned our attention to the two individuals that we knew were at the store with the missing person's vehicle, and asked them when they had last seen the missing person, and what they were doing on the date in question. They both claimed to be at home, and at this point, we presented them with the evidence from the video surveillance which did not align with their story. One of the individuals then confessed that the two of them had murdered our missing person, and led us to discover the truck and the body in an abandoned apartment complex. Without the original lead from the LPR data, because of the location of the truck, it would likely have been a long time before the truck and body were discovered – at which point the likelihood of tracing this back to our two suspects would have been significantly reduced. Unfortunately, criminals do not always present themselves as criminals in advance – the access to this historical data helped us uncover a homicide and bring those responsible to justice."

El Cajon Police Department Rescues an At-Risk Missing Person Using License Plate Recognition Data

LIVERMORE, CALIFORNIA (September 18, 2013) – Vigilant Solutions announces today that El Cajon Police Department used its online investigative tools and historical license plate recognition (LPR) data to locate and rescue an at-risk missing person.

Chief Jim Redman of El Cajon Police Department states, “A 58-year-old man was reported missing to our department. He was considered “at-risk” due to the fact that he was an insulin dependent diabetic and also suffered from other medical problems. The case was challenging as there were no known areas that he frequented; the only information that we had was the license plate of the vehicle he was driving.”

“Police Services Officer Deck was assigned to investigate the case,” continues Chief Redman. “She checked his license plate against our local LPR cameras, and also against our state and regional database systems, but was unable to find any sightings of his vehicle. She then checked his license plate against Vigilant’s LPR database and found three hits on his license plate in the prior two days, placing his vehicle in a parking area of a local trolley stop. Using this information, officers were able to locate the man who was sitting in his vehicle. The man was dehydrated and confused, and was transported quickly to a local hospital. It is because of the availability of this historical LPR data, collected and made available to law enforcement by Vigilant, that we were able to locate this man and bring him to safety.”

Shawn Smith, Founder and President of Vigilant, states, “We often hear stories about how LPR is used to locate vehicles wanted in connection with crimes, and this obviously serves the public good by making our communities safer. But, we also love to hear stories like this where our systems and our data – coupled with good police work – help bring someone safely back to their family. We commend El Cajon for their efforts.”

Deer Park Leverages License Plate Recognition Technology from Vigilant Solutions to Protect its Community

LIVERMORE, CALIFORNIA (AUGUST 27, 2013) – Vigilant Solutions announces today that Deer Park Police Department in Deer Park, Texas is protecting its community with Vigilant Solutions' license plate recognition (LPR) systems and online investigative tools. Purchasing two mobile LPR systems earlier this year, the department is seeing tremendous results and plans to continue its expansion and use of the technology.

Captain Sharon Massey comments, "We had used another vendor's system for some period of time, but began exploring our options as that system became obsolete. In talking to our in-car-video provider, it was highly recommended that we look at Vigilant Solutions. We began our evaluations and found that Vigilant offered the functionality that we were looking for, as well as some unique features that were not offered elsewhere. The availability of additional LPR data from Vigilant and tools to leverage all of this information, such as LEARN and Mobile Hit Hunter, gave us the confidence that we were making the right decision. In hindsight, we have seen great responsiveness and support from Vigilant and they have certainly lived up to their recommendation."

Captain Massey adds, "We deployed our first two systems earlier this year, and they have already paid for themselves. Literally, in terms of the almost $30,000 we have been able to recover related to over 150 outstanding warrants, and more importantly in terms of our ability to take criminal elements off the street. In addition to the warrants that we are now able to enforce, the system has resulted in a similar number of traffic stops including a number of stolen vehicles and other persons of interest. Also, we had a hit-and-run occur where the only lead we had was a partial plate and vehicle description. Searching the system, we saw a match and were able to ascertain a probable location to investigate based on historical data. We located the vehicle at the location, and the driver confessed to the hit-and-run."

"We are looking to expand our use of LPR with additional mobile systems while at the same time following some of the concerns in the media regarding the use of LPR technology. We have a strict written policy that the system is for official and legitimate law enforcement purposes only. All of our officers are trained on the policy and understand the ramifications of breaking policy. We believe that the system is helping us do great work within our community, and our residents should feel good that we have this tool available to help keep our streets safe," concludes Captain Massey.

Residence of Suspect in Officer Shooting and Double Homicide located using Historical License Plate Recognition (LPR) Data from Vigilant Solutions

LIVERMORE, CALIFORNIA (AUGUST 6, 2013) – Vigilant Solutions announces today that its license plate recognition (LPR) data and online investigative tools were used by the Arizona Counter Terrorism Information Center's (ACTIC) Criminal Investigation Research Unit (CIRU) in an investigation connecting the murderer of a Maricopa County Deputy Sheriff to a double homicide.

Sergeant J.D. Williamson of ACTIC recounts the tragic events, "On the morning of January 6, 2012, two individuals were found in their sedan at a remote turnout on Arizona Highway 89A near the scenic resort town of Sedona, Arizona. They were shot with a .223-caliber rifle and several shell casings were retrieved at the scene. Police asked the public to call authorities if they saw what the Police believed was the suspect's vehicle, a 1998 Toyota Sienna mini-van with Illinois license plates, which had been recently seen in the area."

"Two days later, Maricopa County Deputy Sheriff William Coleman, age 50, was shot and killed while responding to a burglary call in Anthem, Arizona at approximately 4:15 am. As Coleman and another deputy arrived at the scene they encountered a male subject inside of a van at a medical building. As they attempted to make contact with the subject he opened fire on them with a rifle, striking Deputy Coleman below his vest. The suspect was killed by return gunfire from other deputies," states Williamson.

Maricopa County Sheriff's Department Investigators then contacted ACTIC in an effort to create a timeline of the suspect's recent movements and locate a current address. Williamson adds, "The vehicle was registered out of state and the suspect was believed to be the registered owner's son. Although much information was gained through law enforcement research systems, CIRU was unable to locate a local address for the suspect because he had only recently moved to Arizona. The license plate was entered into Vigilant Solutions' system of over 1 billion license plates, and this historical LPR data provided investigators with information about the suspect's movements prior to the three homicides. Using this information, we were able to determine a local address that could not be found in any other system. Based on this information, Detectives were able to serve a search warrant on the suspect's residence." Maricopa County Sheriff, Joe Arpaio, said ballistic experts from his office confirmed the cartridges retrieved from both crime scenes were fired from the same weapon.

Deputy Coleman served with the Maricopa County Sheriff's Office for 20 years. He is survived by his wife and four children.

St. Charles Police Department Locates Suspects in University Bomb Threat, Gas-Station Drive-Offs, and Other Cases using Vigilant Solutions License Plate Recognition and Online Investigative Tools

LIVERMORE, CALIFORNIA (JULY 16, 2013) – Vigilant Solutions announces today that St. Charles Police Department in Missouri is seeing benefits from Vigilant's diverse offering of mobile license plate readers, license plate recognition data, Mobile Companion smartphone application, and hosted LEARN enterprise solution for investigations. Most recently, their use enabled the identification and location of a suspect in a bomb threat at Lindenwood University.

Officer Ken Mayer states, "We implemented Vigilant in April of this year, and we had no idea what a success the system would be. Within only weeks of use, we found that the product and service from Vigilant far exceeded our expectations. This is the most useful tool I've seen in my twenty years of law enforcement! At this point, the only problem we have is potential legislation that may limit our access to LPR data…data that is helping us solve and prevent many crimes. We are looking forward to expansion of the system, and are also excited to hear that Vigilant will soon offer a facial recognition solution."

Officer Mayer adds, "In addition to helping find the suspect in a recent bomb threat at Lindenwood, the system has helped us on numerous other cases. In one case, we were looking for a self-confessed meth addict. We ran her plate through the Vigilant system and found it was read ten times in the past two weeks. Using this information, we were able to canvass the area and locate the suspect in a basement where she was placed under arrest. She confessed to stealing cash and currency from her eighty-two-year-old grandmother as well as two gas-station drive-offs."

"In another case, we were working a traffic crash where one of the vehicles left the scene. The suspect left the other party with a first name, license plate number and insurance information. Upon checking the license plate with our Department of Revenue, we found that the license plate belonged to a Kia, while the victim stated the vehicle was a Toyota. The phone number associated with the license plate had been disconnected, and the address of record did not yield any leads. Using Vigilant's mobile app on his iPhone, the officer was able to find historical sightings of the license plate, attached to a Toyota. Shortly afterward, officers responded and found the vehicle parked in front of the apartment complex that the Mobile Companion app had identified."

Sacramento County Continues Successful License Plate Recognition (LPR) Program with Vigilant Solutions' LPR Data

LIVERMORE, CALIFORNIA (June 13, 2013) – Vigilant Solutions announces today that Sacramento County Sheriff's Department (SCSD) continues its successful license plate recognition (LPR) program with Vigilant Solutions's network of private LPR data and online investigative and analytic tools. Vigilant's private LPR data is harvested from a number of sources and made available exclusively to law enforcement for investigative use.

Sergeant Kyle Hoertsch states, "We've enjoyed many successes using Vigilant's products and services dating back to late 2010. Just recently, we received access to additional LPR data through Vigilant's national LPR data network of over one billion detections from around the country. I am amazed both at the amount of data, and the results we have generated. In just the first thirty days of having this data, we located 519 vehicles of interest, including 495 stolen vehicles, 5 carjacking vehicles, and 19 other felony vehicles. Directly related to these vehicles and the crimes, we have been able to take 45 people into custody."

Hoertsch states, "A couple of additional successes involving Vigilant include a takeover bank robbery and a home invasion involving an assault on an elderly woman." Hoertsch continues, "A Wells Fargo Bank in Sacramento was the victim of a takeover bank robbery. A witness was able to obtain the license plate number as the suspects fled. A check of the license plate in the Vigilant system showed one capture of the vehicle on a major highway approximately six months prior. The color photo was shown to the original witness who positively identified it as the vehicle used in the robbery. The color photo was so detailed you could see three distinct bumper stickers and a black bumper on a grey car. Equipped with this detailed vehicle information, officers began canvassing the area and quickly found the vehicle in an apartment complex about a mile from the robbery scene. The suspects were ultimately located and taken into custody."

"In another incident," Hoertsch adds, "we responded to a report of a home invasion. We found a sixty-eight-year-old female tied up; the suspect had forced her to drink alcohol during the crime to a point where she was barely conscious. The suspect fled the scene in the victim's vehicle, however she was unable at the time to provide us with a vehicle description due to her level of consciousness. After locating her license plate number through other methods, we checked the Vigilant system which had three historical detections. These captures provided color photos of the vehicle that featured a very distinct chrome license plate frame that allowed us to locate the vehicle just minutes later with the suspect inside. After a foot pursuit, the suspect was taken into custody. Certain states are attempting to limit the time that historical LPR data can be held when the vehicle is not connected to a crime, but in this case, I am sure that this sixty-eight-year-old woman is glad that her vehicle's picture was taken."

"Vigilant's products, and their data, really help us do our job more efficiently," concludes Hoertsch.

Los Angeles Police Department uses Vigilant Solutions License Plate Recognition (LPR) Data to Locate Suspect in Rape / Sodomy / Beating Case

LIVERMORE, CALIFORNIA (June 4, 2013) – Vigilant Solutions announces today that its license plate recognition (LPR) data and investigative tools were used by the Los Angeles Police Department (LAPD) to locate a suspect in a violent rape / sodomy / beating case.

Detective Patricia Batts of LAPD comments, “We used Vigilant’s LPR data to track the vehicle of a suspect wanted in a rape/sodomy/beating case. Using historical sightings of the vehicle in the Vigilant system, we were able to identify a probable location for the suspect – an apartment complex in Las Vegas. The U.S. Marshals were able to locate the suspect at the complex and he was taken into custody. Had it not been for this data, collected and shared by Vigilant, who knows how long it would have been before the suspect was captured and how many more victims would have been hurt.”

Shawn Smith, President and Founder of Vigilant Solutions, comments, "I am glad that we played a role in locating and apprehending this dangerous individual, and like Detective Batts, I am hopeful that this prevented him from hurting other victims. We applaud the LAPD and the U.S. Marshals in their efforts.”

Large Interstate Drug Cartel Identified with Vigilant Solutions' License Plate Recognition (LPR) Data and Investigative Tools

LIVERMORE, CALIFORNIA (May 14, 2013) – Vigilant Solutions announces today that its license plate recognition (LPR) data and investigative tools were used to identify a significant smuggling organization involving over twenty (20) vehicles being used to transport narcotics across the country.

A police officer in Alabama that works as part of a criminal interdiction task force in cooperation with other agencies and drug interdiction specialists throughout the country used Vigilant Solutions LPR system and historical database to further an ongoing criminal investigation. Earlier this year a vehicle was stopped in the northeast region of the United States, where an aftermarket hidden compartment was discovered that contained a large amount of cocaine worth almost half a million dollars. The officer stated, "I checked the vehicle's license plate against Vigilant Solutions' national network of historical LPR data and saw it had been scanned multiple times, dating back to 2011, at various locations around the country".

The officer continued, "Through further investigation another vehicle was linked to the earlier seizure. I also ran this license plate against the Vigilant LPR data where it had also been scanned in the same areas as the other vehicle. Finding these two vehicles related in terms of location prompted us to do some additional research into these locations. Shortly after this finding, one of the suspect vehicles was stopped in the southeastern region of the United States. This vehicle was also transporting a large amount of cocaine, hidden in a secret compartment.

"The historical LPR data and investigative tools from Vigilant are solely responsible for us identifying locations and over twenty (20) vehicles to date that are a part of this group. Additionally, in just one of our vehicle stops, we were able to seize over nine-thousand (9,000) doses of cocaine and prevent this dangerous drug from hitting the streets...and possibly falling into the hands of a child or precipitating a violent crime. I am confîdent that our investigation, enabled by Vigilant, will result in the identification of many more vehicles, allow us to seize more drugs, and ultimately bring about the downfall of this large drug trafficking operation. I am amazed that some states are considering a ban on this data or are planning to limit its retention – this information saves lives," concludes the police officer.

Woman's Life Saved using Vigilant Solutions' License Plate Recognition (LPR) Data

LIVERMORE, CALIFORNIA (May 8, 2013) – Vigilant Solutions proudly announces today that its license plate recognition (LPR) data and online investigative tools were credited with saving a Florida woman's life.

Detective Dan Cucchi of Coral Springs Police Department reports, "On July 13th, 2011, an eighty-four-year-old resident contacted us to report her forty-nine-year-old daughter missing. There had been a recent death in the family, and after her daughter failed to answer her cell phone for more than a week, the mother became very concerned for her daughter's well-being."

"We immediately logged into our Vigilant Solutions' account and searched historical LPR data for the daughter's vehicle. We found three sightings of the daughter's vehicle in just the prior month, captured by Vigilant license plate readers (LPR) deployed on commercial vehicles and shared with law enforcement, and all three were at the same address in Boca Raton. We immediately drove to the location and located the daughter's vehicle. After making contact with the property management, we were able to locate the daughter's apartment. We knocked, but there was no answer. Concerned for the woman's safety, and with a key provided by property management, we attempted to enter the apartment. Unfortunately the door was latched from the inside. Our Detective called out for the woman and heard a soft moan, at which point – with assistance from property management – we made entry into the apartment," continues Cucchi.

Cucchi adds, "The woman was found on the floor, sick, severely dehydrated, and unable to care for herself. Emergency personnel responded and stated that the woman had been without food or water for several days. Her condition was critical, and she was very near death. Clearly, the information provided from Vigilant saved this woman's life."

Vigilant Solutions' License Plate Recognition (LPR) Locates a Fugitive in Identity Theft Crimes against Ailing and Deceased Veterans

LIVERMORE, CALIFORNIA (March 14, 2013) – Vigilant Solutions announces today that its license plate recognition (LPR) technology was used successfully by the Long Beach Police Department (LBPD) in California to locate a fugitive wanted for identity theft crimes against ailing and deceased veterans.

Detective Andre Sanchez of LBPD's Identity Theft Unit was inundated with cases of identity theft against ailing or recently deceased veterans. "I had around 50 victims reporting that credit cards had been issued, and that vacations and other goods and services had been purchased on credit accounts opened in their names," states Detective Sanchez. "I began investigating these claims and found several common ties to a residential address here in Long Beach. Research on the address pointed us to a registered nurse working in a local Veteran's Administration (VA) Hospital at which all of the victims had been patients. A search warrant was obtained, and the nurse was arrested in the process."

"Due to the magnitude of the case and the number of victims, the nurse was released and no charges were filed at the time in order to allow a case to be made," reports Sanchez. As the case developed, it was discovered that the nurse had fled the area fearing prosecution. "We had no idea where she was," states Sanchez, "and that's when we turned to Vigilant."

Searching over 1 billion LPR records available from Vigilant Solutions, Detective Sanchez was able to locate the nurse's vehicle roughly 2,000 miles away. "We had several sightings of her vehicle in and around Chicago. With the photos provided in the Vigilant system, we were able to verify that it was in fact the suspect's vehicle. The sightings were at retail establishments and malls, and I suspected that she was probably there racking up debt for other victims. I contacted a U.S. Marshal's office in Chicago, and she was arrested and extradited back to California, where she pled guilty," concludes Detective Sanchez.

Vigilant Solutions' License Plate Recognition (LPR) and Public Safety Data Systems Are Helping to Fund Improvements in Local Communities

LIVERMORE, CALIFORNIA (February 5, 2013) – Vigilant Solutions announces today that improvements in its public safety data systems are helping to fund improvements in local communities. Vigilant's public safety data systems, which incorporates license plate recognition (LPR), are used by thousands of agencies every day to provide improved officer safety, enhance investigations, locate Amber Alerts, and more. Now, they are helping communities to improve safety and overall quality of living.

Constable Mark Vojvodich, of Bexar County Precinct Three, is responsible for an area that includes seven municipalities and unincorporated areas including San Antonio covering some 319 square miles and a population of over 630,000 residents. One of his primary duties is the enforcement of outstanding Justice of the Peace (JP) Warrants which currently amount to over $95 million in his county alone. "Fines discourage unsafe driving habits – habits that are proven to endanger lives and property," comments Vojvodich. "The goal of enforcing these fines is to place a consequence on the shoulders of those committing offenses, in hopes that this will drive voluntary compliance of our laws over time and result in safer roadways and lives saved. Many do not realize that these JP Warrants can offset property taxes and help fund better schools, improved infrastructure, and other items that benefit the community as a whole."

Constable Vojvodich began using LPR as a way to aid in his enforcement efforts stating, "LPR improves my ability to do this duty while also making it more convenient for those with outstanding warrants. I must have researched, spoken with, and / or trialed at least six or seven vendors. We selected Vigilant based on superior performance, great customer service and responsiveness, and because of unique features that no one else provided."

"The benefits of using LPR for real-time in-the-field warrant enforcement go far beyond the efficiency gains for my Office and the benefits to the County and its residents. Our system for enforcing actually benefits the citizens with the outstanding warrants by offering up a 'friendlier' interaction. Our office is equipped to take payments in the field, and the majority will either make payment or arrange for payment with our officers. Not only is this extremely convenient for the citizen, but it also provides them with a way to stay out of jail, avoid missing work, and avoid vehicle impound fees and other costs that they would incur under more traditional enforcement methods."

"And we aren't simply looking for warrants. We are also using the system to simultaneously watch for stolen vehicles, felony warrants, Amber Alerts, sex offenders in places where they should not be, and other persons of interest. We have numerous examples of our LPR system leading us to more serious criminal offenses involving weapons, narcotics, and more." Vojvodich concludes, "I'm very happy with the results, the service and the support we are receiving from Vigilant."

Vigilant Solutions License Plate Recognition Data Aids in Locating a Child Abducted by an Illegal Immigrant

LIVERMORE, CALIFORNIA (February 4, 2013) – Vigilant Solutions announces today that its license plate recognition (LPR) data was used in helping to locate and recover a missing child in an Amber Alert. The child was abducted by an illegal immigrant.

According to the Maryland State Police, on August 14, 2012, a fifteen (15) year-old girl was abducted from her home by Edgar Daniel Mazariegos-Cifuentes, a forty (40) year-old illegal immigrant from Guatemala illegally residing in New York. Mazariegos was a close friend of the victim's family, frequently visiting the girl's home, and communicating with the girl for approximately one year prior to the abduction. Following an argument with her mother, the girl called Mazariegos because she was upset.

Mazariegos abducted the girl the following day, telling her that he was taking her to see her uncle in Boston. When the girl attempted to call her uncle, Mazariegos took her phone away and told her that he was taking her away to begin a new life together. Mazariegos then drove her to Maryland where he checked them into a hotel and forced her to have sex on multiple occasions over an eleven (11) day period.

Aided by license plate recognition data from Vigilant Solutions, a task force consisting of Maryland State Police Child Recovery Unit officers and others located Mazariegos and the victim in the apartment. Mazariegos later plead guilty to transporting a minor to engage in sexual activity.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Vigilant Solutions Improves Road Safety in Jonesboro

LIVERMORE, CALIFORNIA (October 16, 2012) – Vigilant Solutions announces today that its mobile license plate /number plate recognition (LPR / ANPR) product is used by the Jonesboro Police Department in Georgia to improve road safety.

Jonesboro Chief of Police Franklin Allen states, "I was a non-believer; I was a skeptic. I simply did not believe that the system could do everything I was being told it could do. I had heard negative comments about LPR from surrounding agencies using other competitive systems, and this tainted my view of the technology." Chief Allen's opinion quickly changed.

"We set up a trial of the system early this year. We got into the vehicle and pulled onto a 6-lane highway. Within the first 5 minutes we had 3 hits," comments Chief Allen. "I was impressed but not yet convinced. We kept the trial in operation for 30 days, and after reviewing the statistics and getting general feedback from my officers, I realized that we had found a real game changer. The officers loved the system and commented on its ease of use, and the results that we saw in those first five minutes were not out of the ordinary."

Chief Allen continues, "I saw a great opportunity to address an issue that I feel strongly about. There is a problem around the country of drivers without insurance, suspended registrations and expired tags. This population of drivers presents a safety threat to other law-abiding citizens using our roadways. These drivers tend to have a greater likelihood of being in accidents or being involved in other mischief. And when someone is involved in an accident with an uninsured driver, there are financial consequences for all of us."

Jonesboro deployed its first system in May and began monitoring license plates against various criminal databases such as the National Crime Information Center (NCIC) and local City warrants. In addition to these criminal databases, Jonesboro also deployed hotlists for uninsured drivers and drivers with suspended registrations or expired tags. In just two months, using the Vigilant LPR system, Jonesboro identified over 300 of these types of violations. "In addition to enforcing these violations and improving the safety for other drivers, these types of violations also carry a fine. Our City has a 60-65% collection rate, so the system literally paid for itself in the first 2-3 months. Based on these results, we just approved purchasing our second Vigilant system." concludes Chief Allen.

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Vigilant Solutions Enables Data Sharing in Connecticut

LIVERMORE, CALIFORNIA (August 28, 2012) – Vigilant Solutions announces today that its Vigilant system is used by the Connecticut Capitol Region Chiefs of Police Association (CRCOPA) to facilitate a multi-agency data sharing initiative. The program , hosted by Newington Police Department, now collects and shares license plate recognition (LPR) data from almost a dozen agencies in the region.

The system was conceived in late 2009 when Newington and neighboring Wethersfield began discussing the need for LPR technology. "We had heard many great stories about how LPR brought great efficiencies to an agency, and we wanted to insure that we had the best solution available for our officers and the communities we serve. We also wanted to insure that the system would be completely interoperable with other agencies in the region regardless of vendor," states Chief of Police Richard Mulhall.

A number of systems were reviewed and evaluated, and Vigilant was chosen due to its functionality, ease of use, data sharing and interoperability with other vendors. The initial mobile LPR unit was installed in early 2010 and was used to patrol a major shopping area as well as two major highways coming through the region. After seeing success, Newington brought on additional systems of their own. Other agencies in the region also began adopting Vigilant LPR as well, and all data is shared among the participating agencies to enhance their investigative reach.

Now comprised of over twenty mobile systems that have scanned over 4 million license plates, the system is providing excellent results. Chief Mulhall adds, "By the end of August we will have scanned close to 2 million plates this year with great results. This has resulted in 669 motor vehicle charges and 10 criminal arrests; unregistered vehicles, vehicles without insurance, stolen vehicles, vehicle associated with the terrorism watch list and drugs. We could not have these same results without the Vigilant system." The captured data is also used for investigations and has resulted in a number of recent cases being solved including arson, robbery and a sexual assault of a minor. "The experience has been very positive with Vigilant. The technology works, the Company is easy to work with, and we are seeing a tremendous benefit," Chief Mulhall concludes.

Deputy Chief Beau Thurnauer of nearby East Hartford Police Department echoes Chief Mulhall's comments, "Since its inception the LPR program has not only exceeded our performance expectations but has without question been the smoothest regional effort I have ever seen. Vigilant has made the installation painless, stayed right on budget and continues to respond quickly to every concern we have. I have never seen the level of support from a vendor as I have seen in this case. This will prove to be the most important technology endeavor I have witnessed in 35 years on this job."

Editorial contact:
Brian Shockley, +1 (925) 398-2079 ext 731, brian.shockley@vigilantsolutions.com

Real-World Examples of the Importance of Historical and Privately Collected LPR Data for Law Enforcement Investigations

BACKGROUND: It is helpful to understand the benefits of historical and privately collected License Plate Reader (LPR) data first-hand from law enforcement investigators who use this data to solve crimes. Below is a small selection of narrative responses received from law enforcement personnel nationwide who use LPR technology as well as historical and privately collected LPR data to break cases and solve crimes. Misspellings and basic grammatical errors have been corrected for readability.

Protections against misuse of LPR data are worthy of consideration, but the following examples indicate that the debate about LPR should be focused on how to get the tool in law enforcement's hands more quickly, rather than how to limit its use.

NOTE: NVLS stands for National Vehicle Location Service and is a nationwide data sharing initiative from Vigilant Solutions. The LPR data being contributed to the NVLS initiative is comprised of data shared by law enforcement agencies and made available (exclusively to law enforcement) free of charge. Vigilant also maintains data from private LPR collection sources and makes this available for analytic use within its LEARN software suite.

Case Examples of Historical and Privately Collected LPR Data Being Used to Solve Crimes

From the NetChoice survey of Vigilant Solutions users:

"We had a bomb threat at a local junior high from an ex-student. We didn't know where he was living but we did know what kind of car he was driving and the license plate. We were able to scan our records for the past year (since the beginning of our LPR installation) that allowed us to hone in on a section of our city where we not only found the vehicle but also our suspect 4 blocks from the school he threatened."

"One of our sister agencies had a murder that went unsolved for several months. A detective accessed the LPR database, and located the murder suspect vehicle based upon location of the LPR hit. This murder would have more than likely gone unsolved without having the old LPR data."

"There was a case in a Florida sheriff's department that resolved 30 rapes over a 3-year period working from a partial plate and partial vehicle description."

"We had an individual that was stealing wallets from businesses and using the victims' credit cards all over the state. I identified the vehicle he was using, and when I ran the plate through our LPR it showed that 6 months prior the suspects vehicle was captured on our LPR in front of a business that had another wallet stolen. When we checked the video for the wallet theft it was the vehicle driver, he was charged and arrested."

“We had a cold case fugitive wanted for murder and nothing else identified where he or his girlfriend was. We got a historical hit on her car and after surveillance he was arrested for the murder.“

“During the Boston Bombings, we used this data to find possible sites within our jurisdiction that might have suspects’ connection.”

“I used it for a double homicide investigation and was able to track down the vehicle using historical data. Both suspects were captured and are awaiting trial for capital murder.”

“Historical data is very important. I use it with crime series. In one case, after about 30 residential burglaries, a witness got a plate. I went back to the other burgs and found that vehicle had been in the area of several.”

“As an investigator in the property crimes unit, my cases may be ranked on the lower end of the spectrum but it is commonly known that criminals don't stick with only one type of crime. In one of my cases, I was investigating a string of grand thefts occurring throughout the city and had the license plate of a suspected vehicle. DMV did not have a current address for the vehicle or the owner, as the address listed for both was a vacant address. I was able to use the system to locate the vehicle, leading to the arrests of six people (4 were arrested at the residence with multiple items of stolen property and 2 were arrested during the commission of a grand theft after we were able to conduct surveillance on the vehicle). The information provided was dated 2-3 months prior to the date I entered my search query.”

“An informant stated that a murder suspect was seen with an unknown female in a specific vehicle and had a license plate number. The registration name and address were incorrect. NVLS showed the vehicle parked at a different motel every couple of days in a certain area of the city. It took very little searching and surveillance to locate the vehicle and observe the suspect in the motel. A warrant was issued and the suspect was arrested without incident.”

“Historical LPR data was used to locate a suspect vehicle in a residential burglary. The vehicle had been seen by the ALPR three months earlier and we were able to match the vehicle to the crime due to the partial plate obtained by the witness and matched the description of the vehicle with the previous LPR scan.”

“While working on a murder case, we received information that the suspects acquired a rental vehicle to commit the murder. Using LPR historical data, we found that vehicle to be within a 1/4 mile of the murder location right before the time of the murder.”

“I use LPR for all of my drive by shooting cases and it has assisted me on my gang cases consistently. One recent case was a known gang member who had beaten, robbed, and left the victim naked in the alley. Through the use of LPR I was able to track his car in a location (months prior) that showed it parked on a couple different occasions. The suspect lived in a different city but his LPR hit showed him in our city. As we were canvassing the city attempting to locate his car I accessed the LPR system for his car. We drove to the area of the LPR hits and located and arrested the suspect who was parked in the exact location of the previous LPR hits.”

“Several times we have used the system to locate a suspect's residence when it is known they are not residing at what is listed on their drivers license or registration. Historical

information was used to identify the apartment they were living at. Also has been used to locate suspects who are staying at long term motels."

"The time frame of when a suspect and suspect vehicle may be identified in a major case for a year or more. If the location data of where the suspect vehicle had been seen a year prior was no longer retained it would be impossible to place where the suspect may have been or where to go look for the suspect."

"A safe house used to facilitate human trafficking was located through LPR data several months old, because the subject, who suspected he was being observed, discontinued direct contact with the safe house."

"A vehicle burglary occurred in our city in which a vehicle used to replenish area ATM machines was broken into and a large sum of money removed. Incident was captured on a business surveillance camera and suspect vehicle was listed, but no plate. A speed camera captured a van with Georgia tags, but leads went cold when most of the suspects involved were [determined to be] illegal aliens. A search of the system led detectives to Queens, NY were the vehicle was spotted and later led to the arrest of a suspect in this investigation."

"I have recovered 10 stolen vehicles in a 7 day period all from private data collection through Mobile Hit Hunter. Those people [who had their cars stolen] were thankful for [the privately collected historical LPR data]..some vehicles were reported stolen over 2 months prior to recovery."

"Gang shootings that occur throughout a long period of time at numerous locations and in different jurisdictions can be linked with the retention of these records."

"My partner worked a missing person case in which the family of the elderly missing person had lost contact with them and did not have a recent address for them. All of our other resources yielded no results, but a check of the system led him to an apartment complex where her vehicle had recently been parked. She was then found and had suffered a bad fall, seriously injuring herself. She had been unable to walk, eat, or drink for days and was very near death at the time she was found. Without the use of NVLS, she would have certainly died."

"LPR tracked large scale cocaine trafficker to an area where he resided. Resulted in millions of dollars of cocaine being seized and prevented it from hitting the street."

"I was involved in a human trafficking case where LPR data placed the suspect's vehicles at various locations around the country. That data helped find people that were being hidden."

"NVLS helped our agency locate a child molester who changed addresses frequently. Without it we would have never located him."

"A murderer's vehicle was confirmed months after the crime when a possible suspect was developed. He had since crushed the vehicle. A check of the database revealed a picture of the vehicle and the distinguishing features that helped confirm it was the correct vehicle."

"A suspect was involved in a homicide in one city and the marker plate was obtained by witnesses. The LPR tracked the suspect car through several cities and an address associated

with the suspect was obtained in the last city recorded. The suspect was found at the address and arrested. No way that would have been done without the LPR data."

"In a case where an illegal alien male subject, who had been previously deported, was accused of statutory rape and child molestation of two sisters, victim/witness testimony assisted me in tracking my fugitive in Alexandria, Virginia. The incident occurred in Dekalb County, Ga. With this information and the assistance of ICE and the US Marshals, the subject was located, taken into custody, and extradited to Georgia for prosecution. Without NVLS, this subject who clearly attempted to elude law enforcement would probably have never been caught."

"We received information a year after a homicide about a suspect. Use of the LPR system was able to place the suspect's vehicle in the area a few days before the homicide."

"LPR data is frequently used in my jurisdiction to identify involvement in homicides and major crime scenes. As a result of LPR access, numerous crimes have been solved and suspects identified and apprehended due to law enforcement's ability to query LPR data, including data that is several years old."

"Suspects to many major crimes are not identified until days, weeks, months and sometimes years later. It's not until that time that LPR data can be searched for links to the crime being investigated or other crimes that we may not have even been aware of."

"[One case involved a] long-term stolen car that was recovered after 6 months. The company did not make the report for an extended period of time and I was able to track it via the LPR database. Never would have recovered it without that."

"Recently I was working a missing persons case that was over a month old. A suicidal female had left her child with family members and was not heard from since. I checked the system for a plate that I had located in old records from 2 years ago and was able to find the plate had been scanned about 8 months prior to my case, in a city 40 miles away. I was able to contact that agency who provided me with newer information which lead to a city adjacent to mine. In contacting the neighboring agency we were able to locate the missing female, alive, the same night I contacted the agency. Without the information it is likely I would not have learned of this case-closing information."

"I have used historical data to help identify the patterns of violent drug dealers."

"The data is often used in our agency for cold case homicide investigation. By nature, such cases are "older." Because historical data is stored and is searchable, this is an invaluable tool."

"In New Jersey there was a shooting which resulted in two injuries. The NJ license plate was known, but address was old. When LPR data was queried, the vehicle was located 4 of 5 nights outside the same address in New York City. A surveillance of the location, coupled with additional public information, provided enough information to locate the individual and make an arrest."

"Recently, I tracked a team of illegal immigrants that were burglarizing businesses, stealing business checks, forging and cashing them all across the southeast United States. They stole

more than $2 million before I'd discovered their pattern. These criminals had multiple aliases and made a point to trade vehicles in at used car dealerships every two weeks. If it weren't for LPR data, I would not have been able to track and apprehend them. All but one of the suspects were captured in Illinois. The other suspect was captured in Texas, on his way to Mexico, after an officer got an LPR hit on his tag."

"Recently a burglary suspect was spotted in a nearby city using historical LPR data, this led to us determining a family member there was helping to fund and hide the suspect. We had been having trouble locating the suspect, and without LPR data we would've never know where the suspect was located."

"I recall a stolen vehicle ring where the bad guys were re-plating high end stolen vehicles such as BMW, Mercedes, Audis, etc. They were utilizing dealer tags that came back to a bad address. We utilized the LPR software to find out where the vehicles were being parked and followed the leads and eventually broke up a large million dollar stolen vehicle operation in the Metro DC area."

"Bank robbery occurred. Vehicle license plate is collected at scene of crime from witness. Plate number is entered into reader. Historical data shows the vehicle parked in front of same house, different from DMV data, on several different days. Officers respond to area and find the car and subsequently arrest robbery suspect."

From press releases, letters of support, and other sources:

"A murder occurred at a liquor store at 4th and Cherry. Two males enter the store and one approached the counter and pointed a 357 Magnum handgun at the clerk and demanded money. The clerk decides to try and call the police and the gunman shoots the clerk in the head, killing him. Both suspects run out of the store and enter a dark colored Nissan Maxima and drive northbound Cherry. One of the responding units equipped with an ALPR captures the license plate as the vehicle drives away from the scene. Later on in the investigation the plate is discovered for the get-away vehicle. Not only did the responding unit capture the vehicle leaving the immediate area (with the ALPR), but prior months and hits almost a year old lead detectives to locations not only in the city of Long Beach, but also into the County of Riverside, CA."

"A body dump occurred on the Westside of Long Beach. The victim was shot and his body was wrapped in a blanket and dumped in an alley. Very little clues and leads were known at the beginning of the investigation. Months later, a license plate and description of the vehicle was given to detectives, they were able to determine that the suspect vehicle was not only in the area at the time of the body dump, but also photographed several months earlier at the location where the murder took place. This was a long investigation that led detectives to the cities of Granada Hills and Chico, CA and ultimately to the arrest and conviction of multiple suspects."

"A shooting occurred at a high school football game between two rival gang members. Unfortunately a cheerleader was caught up in the exchange of gunfire and was shot and killed. Homicide directed detectives to locate a key witness to the shooting. A license plate and vehicle description was given to help locate this witness. Detectives drove to the registered owners address listed with the Department of Motor Vehicles and we unable to

locate the vehicle for several days. Several ALPR hits were discovered at an address in the City of Long Beach over a one year period. A detective performed surveillance on that street until the vehicle arrived on scene. Because that witness was located and brought to court, all suspects involved were sentenced to life in prison."

"A shooting occurred in which and ex-girlfriend set up her child's father to be killed. The victim was lured to the murder location by his child's mother, when he arrived in front of her apartment, a gunman appeared and shot the male to death in his vehicle. Homicide conducted their investigation over several months that led homicide detectives to Las Vegas, NV to arrest the female who set up the murder and gave homicide detectives the name of the shooter. Detectives were able to determine the suspect's vehicle and license plate number. They ran the plate through the ALPR because we could not locate the vehicle at the registered owner's address. ALPR hits over several months led us to a location where we were able to locate the vehicle and take the suspect into custody."

"Gang detectives driving a ALPR equipped plain car were preparing to make a left turn when the past a vehicle in the number two lane. Unbeknownst to them, the ALPR system grabbed a photo of the vehicle and the license plate as the past. Less than a second later, the passenger of that vehicle opened fire on the detectives striking one of them and their vehicle. Officers in the area returned fire and the vehicle sped away. Detectives were able to confirm the suspect vehicles description and plate using the ALPR read obtained by the system. The suspects were ultimately arrested."

"A crime report was taken in North Division for a robbery involving a juvenile Compton gang member. At the time of the incident the victim saw the suspect get into a vehicle and drive away. The victim wrote down the license plate number. It was later determined the R/O of the vehicle, which at the time was registered to a Long Beach address, was the suspect's mother. With the use of the ALPR, detectives were able to locate the vehicle in Compton, ID her son, conduct a show up, and arrest the suspect. The ALPR read was also use in court to prove the location, date, and time of the vehicle when the robbery took place. An ALPR vehicle had just driven by the suspect's vehicle which at the time was parked in the area prior to the robbery. The suspect was found guilty with a gang enhancement."

"Homicide was called to the scene of a murder where the body of a female college student was bound and stuffed in a closet. She had been there several days before being discovered by family members checking her well-being. During the investigation that followed, detectives spoke with the victim's boyfriend who denied seeing the victim the day she disappeared. Detectives were able to use ALPR and show that his car was parked in front of her apartment the day detectives think the victim was murdered. This was compelling evidence to confront the boyfriend with and he ultimately confessed to the murder."

"CHP had attempted a traffic stop of a white Chevy Tahoe, with custom rims and bogus paper dealer plates on it. Unbeknownst to the CHP officer the occupants of the car had just committed an armed bank robbery in Orange County. While the officer was approaching the car one subject exited the car and fled on foot while another front passenger drew a firearm and shot at the CHP Officer from the car. The CHP officer returned fire striking the Tahoe, but the suspect vehicle drove off and successfully eluded capture. Assisting units were able to set containment and arrest the subject who had fled on foot. This subject was ultimately arrested for his participation in the bank robbery in Orange County, but he would not identify the passenger who shot at the CHP Officer. Detectives then started running ALPR

reads in month long batches around his known associates and his known addresses. It was through this process they found a white Chevy Tahoe with custom rims and a license plate on it. Based on the ALPR hit, Detectives located the Tahoe, which had been repaired by the time they located it. Detectives had a body shop cut holes in the passenger door where they found bullets, which were ultimately matched to the CHP Officers weapon. This tied the Tahoe to the shooting and led us to identify the suspect. The suspect was ultimately convicted of the armed bank robbery and is still awaiting trial for the attempted murder of a police officer."

"A male subject wrapped in bedding material had been dumped in the alley with a single gunshot wound to his head. The victim had been stripped down and there was no identifying information on him. After a lengthy investigation which included numerous search warrants, Detectives identified several numbers the victim had called the day of his death using the victim's phone records. Through this process they identified a subject who the victim had called several times just before his murder but the subject had his phone turned off, preventing officers from identifying where he was at the time of the murder. However, Detectives identified a black 4-runner registered to the subject's wife. When they ran this plate through ALPR, they found the 4-runner parked directly in front of the crime scene just a few minutes before the murder. Later a witness would tell Detectives that the victim had been shot in the head and loaded in the 4-runner when a patrol officer drove by capturing the plate in the ALPR system. "

"Neighbors reported they had not seen the victim for a extended period of time and desired units to check the victim's well-being. Inside they found the body of an adult male in advanced stages of decomposition. As investigators worked through this case and tried to determine what happened, ALPR was crucial for verifying information being given to them."

Additional Law Enforcement Comments Regarding LPR

(Victims assisted, lives saved, suspects exonerated or eliminated, general notes of support – from the NetChoice survey responses)

"There has never been such a useful law enforcement tool on the market that utilizes zero personal identifiable information to operate. A license plate does not tell you who is operating a vehicle or how long they are operating a vehicle. It doesn't provide name, date of birth, social security number or even the address of the subject. LPR data, as a single factor, is a pointer at best. It could only work adequately when coupled with an existing, regulated and monitored database such as State DMV, public record or NCIC."

"Also, keep in mind that plate data can also clear people from crimes. It can prove they were NOT at the scene but somewhere else."

"It is not the collection and storage of data that is bad or potentially bad, it is the misuse of that data that causes the problem. Focus on the violator. It is much like having a vehicle capable of exceeding the speed limit. The focus is on the driver violating the speed limit, not the vehicle being used to do so."

"If people are truly afraid of misuse of the data, outlaw the misuse or add criminal enhancements to other crimes for using LPR data to commit them. Don't take away this valuable tool."

"Records for reads should be kept for as long as possible so that they may be used as historical data in long term investigations or cases such as murder with no statute of limitations."

"While investigating a multi-victim rape case, one of the victims was forced to move from her residence and was not able to pay her cell phone bill, causing her cell phone to be deactivated. She moved into a motel in a different part of the county. The court case had been delayed for well over a year and the victim had severe health issues. The simple task of notifying the lead detective of her new residence was not the first thing on her mind. Thanks to her vehicle's license plate being scanned into the LPR system, we were able to locate this victim and notify her of an upcoming court date."

"I do know that historical "scan" data is as important or in some cases more important for investigations than the data involving "hits." With the back log of subpoena processing centers and the slow responses from cellular phone companies to law enforcement requests most investigations take a considerable amount of time to develop leads where there are none initially. Leads developed that point to a particular suspect where an investigator can determine a possible license plate on a vehicle used the historical "scan" records may place the suspect coming or going from the scene of a crime or multiple (serial) crimes. Being able to show where a possible suspect was on a map with an image of the license plate (and sometimes rear of the vehicle showing a distinguishable sticker) to a jury at trial is a game changer for law enforcement."

"Criminal investigations can take months to work. If we cut ALPR databases to days and weeks, the valuable vehicle info we obtain months into and investigation would be useless when trying to prove a certain vehicle was in a certain area during a certain time period."

“Historical LPR data is extremely useful in tracking and locating criminals. Perhaps the ACLU would rather have a wanted rogue criminal or sex offender at large, in their neighborhood, unable to be tracked or located by law enforcement, with the only means of location being when that criminal or sex offender struck again and victimized another innocent child or family member.”

“Unidentified murder victim - LPR data showed history of visits to locations which led to victim identification and ultimately an arrest.”

“[LPR is a] success. Criminals go to great lengths to hide their location from LE officers. LPR saves officers time during their investigation, and saves the department money by avoiding unnecessary time being spent trying to locate a suspect. This system has even assisted us with locating unknowing victims of crime, who did not have their current address listed on their vehicle registration and/or driver's license. A more accurate report should indicate the number of searches for plate scans conducted by users, and the number of hit returns.”

“A woman's adult daughter was missing after her Dad passed away. The daughter did not take the loss of her Dad well, moved away from where Mom knew her to be and stopped calling her Mom. The daughter was located due to LPR scans and had fallen in her apartment 3 days earlier, unable to move or call for help. EMS and doctors estimated she may have lived another 12-24 hours before her death had we not found her and saved her life.”

“LPR data is used in our Agency frequently to include or exclude a possible vehicle match based on color. If a Victim provides a license plate and said the vehicle was red, and the LPR capture shows the vehicle as white, we know the Victim gave the wrong plate. DMV date does not provide vehicle color.”

“Historical information is so valuable in cases where the crimes we investigate have Statutes of Limitations of 10 years.”

“I understand the need for taking the steps to assure citizens’ rights are protected but, this system works. There is always someone in any company or organization that could abuse their authority/position including the ACLU. I feel an audit is a reasonable and fair solution. To erase data days or weeks after crimes is not in the best interest of public safety.”

From: PoliceOne Roll Call
To: McCarthy, Steven (POL)
Subject: 1 dead in Wash. school shooting; How to help Irma responders
Date: Wednesday, September 13, 2017 5:13:53 PM

September 13, 2017 | View as webpage

Print for Roll Call | Download the Mobile App

Dear PoliceOne Subscriber,

While our nation comprehends the devastation caused by Hurricane Harvey, responders have been dealing with the aftermath of Hurricane Irma. Our thoughts are with all the law enforcement, firefighting and EMS personnel currently working on rescue and relief efforts.

For information on how to help Hurricane Irma first responders, see this list of charitable funds specific to public safety.

For readers impacted by Hurricane Irma or who are participating in the response, we invite you to send your photos and stories to editor@policeone.com.

— *The PoliceOne Team*

TOP NEWS

Officials: 1 dead, 3 injured in Wash. school shooting

Berkeley police get to use pepper spray at violent protests

Off-duty Puerto Rico officer fatally shot during armed robbery

DOJ won't bring charges against officers in Gray case: The death touched off weeks of protests and unrest in Baltimore

Calif. police chiefs end opposition to sanctuary measure

Baltimore plans to offer $2,500 a year property tax discount for LE

Retired NY officer dies of 9/11-related cancer: Walter Mallinson leaves behind his wife and two children

Calif. K-9 injured, suspect shot after pursuit: The suspect rammed his truck into a gate and parked patrol car at a Sacramento police substation

Sheriff who threatened arrests at Irma shelters is sued

Video: Fla. officer saves fallen flag from middle of road after Irma

Thompson submachine gun nets $90K for sheriff's office at auction

Robbery suspects run into police station while fleeing

ELSAG is Now LEONARDO!

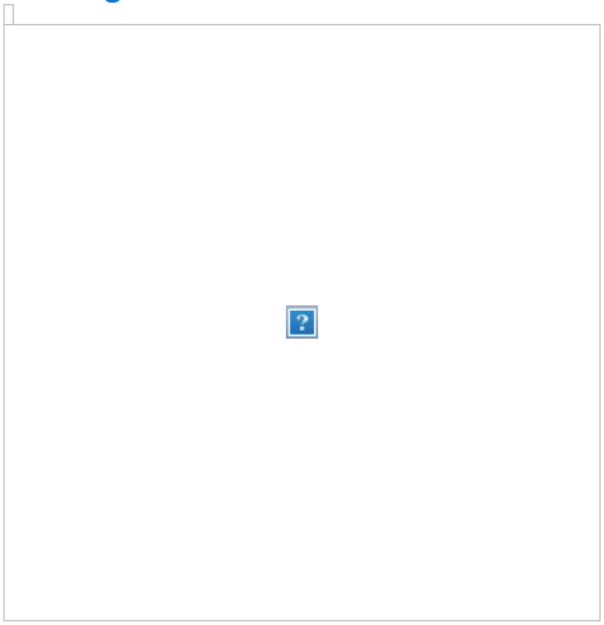


We're changing our brand! Over the coming months, when you see the LEONARDO brand mark, know that's us. Visit LEONARDO at IACP booth #1937 to experience our advanced ALPR technologies.

Witness the change

COMMUNITY POLICING

6 things cops should do before running for office

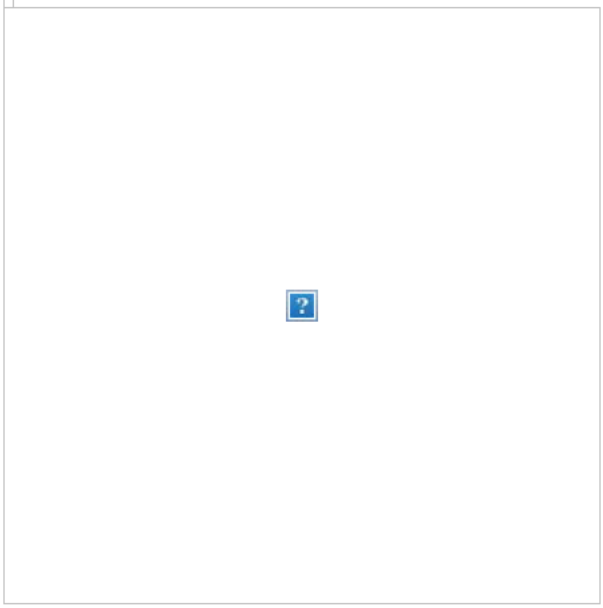


By James Spadola, PoliceOne Contributor

There is no reason law enforcement officers

TECHNOLOGY

How criminals are using 3D printing



By John Hornick, PoliceOne Contributor

Criminals are using 3D printing to make guns, reproduce keys and manufacture illegal drugs.

have to remain on the sidelines of democracy.

Trust yourself

Changing the game

PRODUCT VIDEOS

Vigilant Solutions Explainer
Developing investigative leads is critical to fighting crime whether you're in the office or in the field.

PRODUCT NEWS

NRA National Police Shooting Championship returns to Albuquerque this September

ATS Armor LLC enters the soft body armor market

More Product News

FEATURED DEALS

One-Click Video Redaction
See one-click video redaction from MotionDSP

Lynx T4-8 Interior Light Bar
Only $167.96 from Extreme Tactical Dynamics

More Featured Deals

POLICE TRAINING

5 felony traffic stop tactical tips for police officers

By Duane Wolfe, PoliceOne Columnist
The end of a pursuit can be hectic and chaotic so remember to control yourself, trust your training and do your tactical breathing.

PATROL ISSUES

2 traffic stops, 2 very different outcomes

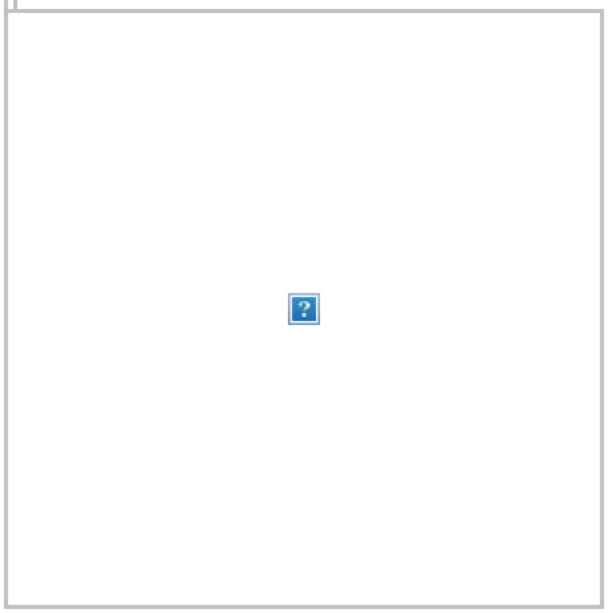
By Charles Remsberg, PoliceOne Columnist
What made the life-and-death difference between two traffic stops on the same offender?

Critical behavior differences

Practice with your partner

FIREARMS

Quiz: Are these long guns and sub-guns real or fake?



By PoliceOne Staff

Police departments have long warned the public about the dangers of replica guns.

Take the quiz

Public Safety's New Standard for Data Collection



SceneDoc's electronic citations tool works with off-the-shelf mobile devices to cut costs, boost efficiency and provide better intelligence to the officer and agency.

Get your FREE demo

MORE ON POLICEONE

Video: LEO assists Kristen Bell during Hurricane Irma shelter performance

NY cop who moonlights as model walks in 1st NY Fashion Week

5 Features of Kyocera's DuraForce PRO that Make it the Right Cell Phone for Cops



Check out this cell phone review by PoliceOne Columnist Lindsey Bertomen, where he shares why the 4G DuraForce PRO is right cell phone for cops.

Built for cops

3.3K DOJ won't bring charges against officers in Gray case

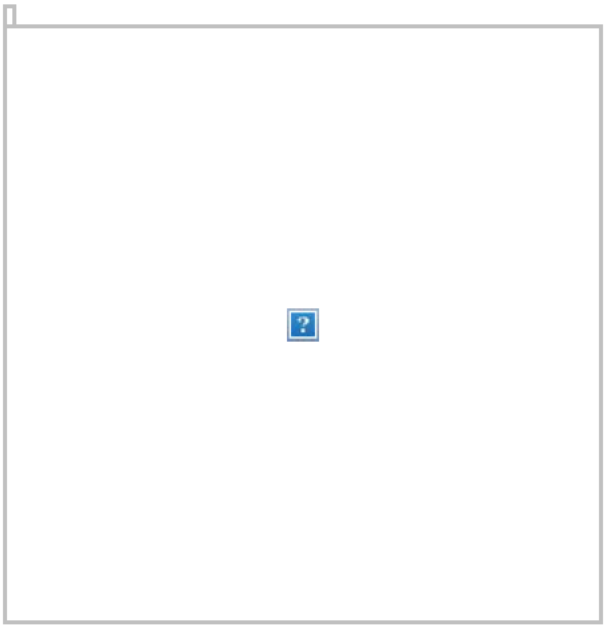
5 things you should know before buying an optic to carry on duty

1.7K Robbery suspects run into Ill. police station while fleeing

1.6K Police: At least 8 dead after shooting in Texas

1K Woman found concealing gun during vaginal search at jail

971 Photo shows Fla. LEO, K-9 passed out from Hurricane Irma response



From quality to construction to ease of use, there's a lot to know before you make your next purchase.

Make an informed purchase

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

This message was sent to steven.mccarthy@pol.state.ma.us from:

PoliceOne Roll Call | Newsletter@policeone.com | Praetorian Digital | 200 Green St Suite 200 | San Francisco, California 94111

Unsubscribe

From: PoliceGrantsHelp eNews
To: Silva, Patrick (POL)
Subject: 2017 COPS Office grants: What police leaders need to know; Grants Help Quick Tip: Always Have A Plan
Date: Thursday, May 18, 2017 6:01:43 PM

May 18, 2017 | View as webpage

Ask a Grant Expert

Dear PoliceGrantsHelp Member,

In this month's eNews, Linda Gilbertson talks about 3 COPS Grant programs you need to know about and consider for funding. While the PoliceGrantsHelp Team provides you with a quick tip video on why it is important to plan ahead for grant success!

Speaking of COPS, are you planning on applying this year? These applications will be opening soon - get a head start NOW with grant writing help from the PoliceGrantsHelp Team. Use promo code **COPS25** before the grant opens to **get 25% off** grant writing services today!

Stay Safe,

— *The PoliceGrantsHelp Team*

FEATURED ARTICLE

What to Do When You Get a Grant Award

Learn what steps you should take to accept and begin implementing the grant

Police grants and sanctuary cities: It's complicated

Learn about the issues of sanctuary cities and law enforcement grants

2017 COPS Office grants: What police leaders need to know

Find Grant Help for Mobile Radios

Need funding

Federal and State Grants Have Funded Many ELSAG Plate Hunter™ ALPR Systems



assistance for Mobile Radios? E.F. Johnson and PGH are teaming-up to lend you a hand.

Get grants help here



ELSAG has partnered with PGH to provide you with services and guidance related to the grant-assisted procurement of our ALPR systems and complementary technologies.

Request grant services

GET GRANT ASSISTANCE

PoliceGrantsHelp offers customized grant assistance in several categories. Click on the links below to access free grant services including: research, consulting and application assistance.

- AEDs
- Boats
- Crime Analysis and Investigation Software
- Explosives Detection
- Firearms Training
- In Car Video
- Less Lethal
- Manned Mobile Surveillance
- Mobile Forensics
- Police Motorcycles
- Radios
- Specialty Vehicles
- Thermal Cameras (EO/IR)
- Training Simulation
- X-Ray Body Scanner
- Airborne Surveillance
- Body Cameras
- Digital Investigation Software
- Fingerprint Biometrics
- Forensic 3D Laser Scanners
- Intelligence Led Policing
- License Plate Readers
- Mobile Command Centers
- Narcotics Identification
- Radiation Detection
- RMS
- Tablets
- Training
- Use of Force Software

ALL GRANTS HELP

POLICEGRANTSHELP EXCLUSIVE

Grants Help Quick Tip: Always Have A Plan

By The PoliceGrantsHelp Team

Learn the importance of planning ahead and getting prepared to get to grant

MORE GRANTS NEWS

- **Firehouse Subs Public Safety Foundation donates equipment to Okla. police**
- **Colo. department receives personal safety grant**
- **Mexico and police chief slam Texas' new**

success

More

'sanctuary city' ban

Va. police department receives grant for life-saving overdose medication

All Grant News

UPCOMING GRANTS

Grant	Grant Deadline
Highway Safety Grant (Louisiana)	5/22/2017
Traffic Safety Grant (Ohio)	5/22/2017
Maryland Body Armor for Local Law Enforcement Grant (BARM)	5/24/2017
Aid to Crime Laboratories (New York)	5/25/2017
State Protection from Abuse Fund (PFA Kansas)	5/26/2017
Pennsylvania Highway Safety Program	5/31/2017
Byrne Memorial Justice Assistance Grant (JAG Ohio)	5/31/2017
Homeland Security Grant Programs (HSGP Virginia)	5/31/2017
Edward Byrne Memorial Justice Assistance Grant (JAG Arkansas)	6/1/2017
Victims of Crime Act Grant (VOCA Missouri)	6/2/2017

Search for more grant opportunities

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

This message was sent to patrick.silva@pol.state.ma.us from:

PoliceGrantsHelp eNews | Newsletter@PoliceOne.com | Praetorian Digital | 200 Green St Suite 200 | San Francisco, California 94111

Unsubscribe

From: PoliceGrantsHelp eNews
To: Conneely, Paul (POL)
Subject: 2017 COPS Office grants: What police leaders need to know; Grants Help Quick Tip: Always Have A Plan
Date: Thursday, May 18, 2017 6:01:43 PM

May 18, 2017 | View as webpage

Ask a Grant Expert

Dear PoliceGrantsHelp Member,

In this month's eNews, Linda Gilbertson talks about 3 COPS Grant programs you need to know about and consider for funding. While the PoliceGrantsHelp Team provides you with a quick tip video on why it is important to plan ahead for grant success!

Speaking of COPS, are you planning on applying this year? These applications will be opening soon - get a head start NOW with grant writing help from the PoliceGrantsHelp Team. Use promo code **COPS25** before the grant opens to **get 25% off** grant writing services today!

Stay Safe,

— *The PoliceGrantsHelp Team*

FEATURED ARTICLE

What to Do When You Get a Grant Award

Learn what steps you should take to accept and begin implementing the grant

Police grants and sanctuary cities: It's complicated

Learn about the issues of sanctuary cities and law enforcement grants

2017 COPS Office grants: What police leaders need to know

Find Grant Help for Mobile Radios

Need funding

Federal and State Grants Have Funded Many ELSAG Plate Hunter™ ALPR Systems



assistance for Mobile Radios? E.F. Johnson and PGH are teaming-up to lend you a hand.

Get grants help here



ELSAG has partnered with PGH to provide you with services and guidance related to the grant-assisted procurement of our ALPR systems and complementary technologies.

Request grant services

GET GRANT ASSISTANCE

PoliceGrantsHelp offers customized grant assistance in several categories. Click on the links below to access free grant services including: research, consulting and application assistance.

- AEDs
- Boats
- Crime Analysis and Investigation Software
- Explosives Detection
- Firearms Training
- In Car Video
- Less Lethal
- Manned Mobile Surveillance
- Mobile Forensics
- Police Motorcycles
- Radios
- Specialty Vehicles
- Thermal Cameras (EO/IR)
- Training Simulation
- X-Ray Body Scanner
- Airborne Surveillance
- Body Cameras
- Digital Investigation Software
- Fingerprint Biometrics
- Forensic 3D Laser Scanners
- Intelligence Led Policing
- License Plate Readers
- Mobile Command Centers
- Narcotics Identification
- Radiation Detection
- RMS
- Tablets
- Training
- Use of Force Software

ALL GRANTS HELP

POLICEGRANTSHELP EXCLUSIVE

Grants Help Quick Tip: Always Have A Plan

By The PoliceGrantsHelp Team

Learn the importance of planning ahead and getting prepared to get to grant

MORE GRANTS NEWS

- **Firehouse Subs Public Safety Foundation donates equipment to Okla. police**
- **Colo. department receives personal safety grant**
- **Mexico and police chief slam Texas' new**

success

More

'sanctuary city' ban

Va. police department receives grant for life-saving overdose medication

All Grant News

UPCOMING GRANTS

Grant	Grant Deadline
Highway Safety Grant (Louisiana)	5/22/2017
Traffic Safety Grant (Ohio)	5/22/2017
Maryland Body Armor for Local Law Enforcement Grant (BARM)	5/24/2017
Aid to Crime Laboratories (New York)	5/25/2017
State Protection from Abuse Fund (PFA Kansas)	5/26/2017
Pennsylvania Highway Safety Program	5/31/2017
Byrne Memorial Justice Assistance Grant (JAG Ohio)	5/31/2017
Homeland Security Grant Programs (HSGP Virginia)	5/31/2017
Edward Byrne Memorial Justice Assistance Grant (JAG Arkansas)	6/1/2017
Victims of Crime Act Grant (VOCA Missouri)	6/2/2017

Search for more grant opportunities

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

This message was sent to paul.conneely@massmail.state.ma.us from:

PoliceGrantsHelp eNews | Newsletter@PoliceOne.com | Praetorian Digital | 200 Green St Suite 200 | San Francisco, California 94111

Unsubscribe

From: PoliceGrantsHelp eNews
To: Deyermond, James (POL)
Subject: 2017 COPS Office grants: What police leaders need to know; Grants Help Quick Tip: Always Have A Plan
Date: Thursday, May 18, 2017 6:02:04 PM

May 18, 2017 | View as webpage

Ask a Grant Expert

Dear PoliceGrantsHelp Member,

In this month's eNews, Linda Gilbertson talks about 3 COPS Grant programs you need to know about and consider for funding. While the PoliceGrantsHelp Team provides you with a quick tip video on why it is important to plan ahead for grant success!

Speaking of COPS, are you planning on applying this year? These applications will be opening soon - get a head start NOW with grant writing help from the PoliceGrantsHelp Team. Use promo code **COPS25** before the grant opens to **get 25% off** grant writing services today!

Stay Safe,

— *The PoliceGrantsHelp Team*

FEATURED ARTICLE

What to Do When You Get a Grant Award

Learn what steps you should take to accept and begin implementing the grant

Police grants and sanctuary cities: It's complicated

Learn about the issues of sanctuary cities and law enforcement grants

2017 COPS Office grants: What police leaders need to know

Find Grant Help for Mobile Radios

Need funding

Federal and State Grants Have Funded Many ELSAG Plate Hunter™ ALPR Systems



assistance for Mobile Radios? E.F. Johnson and PGH are teaming-up to lend you a hand.

Get grants help here



ELSAG has partnered with PGH to provide you with services and guidance related to the grant-assisted procurement of our ALPR systems and complementary technologies.

Request grant services

GET GRANT ASSISTANCE

PoliceGrantsHelp offers customized grant assistance in several categories. Click on the links below to access free grant services including: research, consulting and application assistance.

- AEDs
- Boats
- Crime Analysis and Investigation Software
- Explosives Detection
- Firearms Training
- In Car Video
- Less Lethal
- Manned Mobile Surveillance
- Mobile Forensics
- Police Motorcycles
- Radios
- Specialty Vehicles
- Thermal Cameras (EO/IR)
- Training Simulation
- X-Ray Body Scanner
- Airborne Surveillance
- Body Cameras
- Digital Investigation Software
- Fingerprint Biometrics
- Forensic 3D Laser Scanners
- Intelligence Led Policing
- License Plate Readers
- Mobile Command Centers
- Narcotics Identification
- Radiation Detection
- RMS
- Tablets
- Training
- Use of Force Software

ALL GRANTS HELP

POLICEGRANTSHELP EXCLUSIVE

Grants Help Quick Tip: Always Have A Plan

By The PoliceGrantsHelp Team

Learn the importance of planning ahead and getting prepared to get to grant

MORE GRANTS NEWS

- **Firehouse Subs Public Safety Foundation donates equipment to Okla. police**
- **Colo. department receives personal safety grant**
- **Mexico and police chief slam Texas' new**

success

More

'sanctuary city' ban

Va. police department receives grant for life-saving overdose medication

All Grant News

UPCOMING GRANTS

Grant	Grant Deadline
Highway Safety Grant (Louisiana)	5/22/2017
Traffic Safety Grant (Ohio)	5/22/2017
Maryland Body Armor for Local Law Enforcement Grant (BARM)	5/24/2017
Aid to Crime Laboratories (New York)	5/25/2017
State Protection from Abuse Fund (PFA Kansas)	5/26/2017
Pennsylvania Highway Safety Program	5/31/2017
Byrne Memorial Justice Assistance Grant (JAG Ohio)	5/31/2017
Homeland Security Grant Programs (HSGP Virginia)	5/31/2017
Edward Byrne Memorial Justice Assistance Grant (JAG Arkansas)	6/1/2017
Victims of Crime Act Grant (VOCA Missouri)	6/2/2017

Search for more grant opportunities

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

This message was sent to james.deyermond@pol.state.ma.us from:

PoliceGrantsHelp eNews | Newsletter@PoliceOne.com | Praetorian Digital | 200 Green St Suite 200 | San Francisco, California 94111

Unsubscribe

From: Forensic Magazine
To: Coronado, Elisse (POL)
Subject: ALPR Data Open to Public, California Courts Rule
Date: Friday, September 1, 2017 1:04:29 PM

View this email in your browser.

Forensic News Daily

SEP 01

IN THIS ISSUE

NEWS

Austin Police Partner With UNT Health Science Center

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Crime Alert: chemicals have escaped in your lab

Evidence processing leaves behind a bad smell in your lab. The Halo air filtration system is on the job 24/7 to capture fugitive emissions and return clean air back to the laboratory.

LEARN MORE

FEATURED STORY

ALPR Data Open to Public, California Courts Rule

The automated license plate reader (ALPR) data collected from millions in Los Angeles County is public information, the California Supreme Court ruled this week.

Featured Story

Share

FULL STORY

Ultrafast, Ultra-sensitive GC-MS

Shimadzu's GCMS-QP2020, with the Smart Forensic Database, is the ideal platform for detection and quantitation of targeted drugs in the presence of background interferences.

LEARN MORE

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

Thumbnail

Bodies are piling up at the Houston morgue because of Harvey: Not only did the storm lead to more than 30 deaths, but the widespread flooding has also prevented funeral homes from collecting the corpses of those who died from other causes.

FULL STORY

NEWS

Austin Police Partner With UNT Health Science Center

In the aftermath of its lab's closure, the Austin Police

Thumbnail

Department will now send a majority of its faulty DNA cases to the University of North Texas Health Science Center to determine if retesting must be done.

FULL STORY

Streamlining the Extraction of Drugs Process with Centrifugal Evaporation

Genevac LTD

A method for the extraction of drugs of abuse from urine samples pertaining to drug facilitated sexual assault cases has been developed, involving the use of solid phase extraction techniques prior to screening analysis. Under conventional testing methods, evaporation is achieved using a nitrogen blow down system. This white paper examines the benefits of using a centrifugal evaporation system for drugs of abuse urine sample testing. These benefits include increased sensitivity, reduced cross contamination, and a reduction of time needed to complete the evaporation process.

DOWNLOAD NOW

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Thumbnail

A nurse says she was assaulted and illegally arrested by a Salt Lake City police detective for following a hospital policy that does not allow blood draws from unconscious patients. Footage from University Hospital and officer body cameras shows Detective Jeff Payne and nurse Alex Wubbels in a standoff over whether the policeman should be allowed to get the blood sample.

FULL STORY

NEWS

Pakistan Verdict on Bhutto Assassination Angers Supporters

A Pakistani court on Thursday sentenced two former police officers to 17 years in prison for failing to protect former Prime Minister Benazir Bhutto, but the same court

Thumbnail

acquitted five suspected militants who had confessed to taking part in her 2007 assassination.

FULL STORY

NEWS

Controversial Milwaukee Sheriff David Clarke Resigns

Thumbnail

The tough-talking sheriff of Milwaukee County, David Clarke, resigned without explanation Thursday, capping a tumultuous year for the divisive, provocative lawman whose unabashed support for President Donald Trump and in-your-face personality earned him a national following among some conservatives.

FULL STORY

SUBSCRIBE | ABOUT US | ADVERTISE

We respect your right to privacy - view our policy here.

This mailbox is unattended, so please do not reply to this message. Contact us for assistance.

If you no longer wish to receive these emails - unsubscribe here.

This email was sent by: **Forensic Magazine**
100 Enterprise Drive - Suite 600 - Rockaway, NJ 07866-2129

© 2017 Forensic Magazine. All rights reserved.

From: Forensic Magazine
To: Levasseur, Michelle
Subject: ALPR Data Open to Public, California Courts Rule
Date: Friday, September 1, 2017 1:03:44 PM

View this email in your browser.

Forensic News Daily

SEP 01

IN THIS ISSUE

NEWS

Austin Police Partner With UNT Health Science Center

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Crime Alert: chemicals have escaped in your lab

Evidence processing leaves behind a bad smell in your lab. The Halo air filtration system is on the job 24/7 to capture fugitive emissions and return clean air back to the laboratory.

LEARN MORE

FEATURED STORY

ALPR Data Open to Public, California Courts Rule

The automated license plate reader (ALPR) data collected from millions in Los Angeles County is public information, the California Supreme Court ruled this week.

Featured Story

Share

FULL STORY

Ultrafast, Ultra-sensitive GC-MS

Shimadzu's GCMS-QP2020, with the Smart Forensic Database, is the ideal platform for detection and quantitation of targeted drugs in the presence of background interferences.

LEARN MORE

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

Thumbnail

Bodies are piling up at the Houston morgue because of Harvey: Not only did the storm lead to more than 30 deaths, but the widespread flooding has also prevented funeral homes from collecting the corpses of those who died from other causes.

FULL STORY

NEWS

Austin Police Partner With UNT Health Science Center

In the aftermath of its lab's closure, the Austin Police

Thumbnail

Department will now send a majority of its faulty DNA cases to the University of North Texas Health Science Center to determine if retesting must be done.

FULL STORY

Streamlining the Extraction of Drugs Process with Centrifugal Evaporation

Genevac LTD

A method for the extraction of drugs of abuse from urine samples pertaining to drug facilitated sexual assault cases has been developed, involving the use of solid phase extraction techniques prior to screening analysis. Under conventional testing methods, evaporation is achieved using a nitrogen blow down system. This white paper examines the benefits of using a centrifugal evaporation system for drugs of abuse urine sample testing. These benefits include increased sensitivity, reduced cross contamination, and a reduction of time needed to complete the evaporation process.

DOWNLOAD NOW

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Thumbnail

A nurse says she was assaulted and illegally arrested by a Salt Lake City police detective for following a hospital policy that does not allow blood draws from unconscious patients. Footage from University Hospital and officer body cameras shows Detective Jeff Payne and nurse Alex Wubbels in a standoff over whether the policeman should be allowed to get the blood sample.

FULL STORY

NEWS

Pakistan Verdict on Bhutto Assassination Angers Supporters

A Pakistani court on Thursday sentenced two former police officers to 17 years in prison for failing to protect former Prime Minister Benazir Bhutto, but the same court

Thumbnail

acquitted five suspected militants who had confessed to taking part in her 2007 assassination.

FULL STORY

NEWS

Controversial Milwaukee Sheriff David Clarke Resigns

Thumbnail

The tough-talking sheriff of Milwaukee County, David Clarke, resigned without explanation Thursday, capping a tumultuous year for the divisive, provocative lawman whose unabashed support for President Donald Trump and in-your-face personality earned him a national following among some conservatives.

FULL STORY

SUBSCRIBE | ABOUT US | ADVERTISE

We respect your right to privacy - view our policy here.

This mailbox is unattended, so please do not reply to this message. Contact us for assistance.

If you no longer wish to receive these emails - unsubscribe here.

This email was sent by: **Forensic Magazine**
100 Enterprise Drive - Suite 600 - Rockaway, NJ 07866-2129

© 2017 Forensic Magazine. All rights reserved.

From: Forensic Magazine
To: Heffernan, Kenneth (POL)
Subject: ALPR Data Open to Public, California Courts Rule
Date: Friday, September 1, 2017 1:03:18 PM

View this email in your browser.

Forensic News Daily

SEP 01

IN THIS ISSUE

NEWS

Austin Police Partner With UNT Health Science Center

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Crime Alert: chemicals have escaped in your lab

Evidence processing leaves behind a bad smell in your lab. The Halo air filtration system is on the job 24/7 to capture fugitive emissions and return clean air back to the laboratory.

LEARN MORE

FEATURED STORY

ALPR Data Open to Public, California Courts Rule

The automated license plate reader (ALPR) data collected from millions in Los Angeles County is public information, the California Supreme Court ruled this week.

Featured Story

Share

FULL STORY

Ultrafast, Ultra-sensitive GC-MS

Shimadzu's GCMS-QP2020, with the Smart Forensic Database, is the ideal platform for detection and quantitation of targeted drugs in the presence of background interferences.

LEARN MORE

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

Thumbnail

Bodies are piling up at the Houston morgue because of Harvey: Not only did the storm lead to more than 30 deaths, but the widespread flooding has also prevented funeral homes from collecting the corpses of those who died from other causes.

FULL STORY

NEWS

Austin Police Partner With UNT Health Science Center

In the aftermath of its lab's closure, the Austin Police

Thumbnail

Department will now send a majority of its faulty DNA cases to the University of North Texas Health Science Center to determine if retesting must be done.

FULL STORY

Streamlining the Extraction of Drugs Process with Centrifugal Evaporation

Genevac LTD

A method for the extraction of drugs of abuse from urine samples pertaining to drug facilitated sexual assault cases has been developed, involving the use of solid phase extraction techniques prior to screening analysis. Under conventional testing methods, evaporation is achieved using a nitrogen blow down system. This white paper examines the benefits of using a centrifugal evaporation system for drugs of abuse urine sample testing. These benefits include increased sensitivity, reduced cross contamination, and a reduction of time needed to complete the evaporation process.

DOWNLOAD NOW

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Thumbnail

A nurse says she was assaulted and illegally arrested by a Salt Lake City police detective for following a hospital policy that does not allow blood draws from unconscious patients. Footage from University Hospital and officer body cameras shows Detective Jeff Payne and nurse Alex Wubbels in a standoff over whether the policeman should be allowed to get the blood sample.

FULL STORY

NEWS

Pakistan Verdict on Bhutto Assassination Angers Supporters

A Pakistani court on Thursday sentenced two former police officers to 17 years in prison for failing to protect former Prime Minister Benazir Bhutto, but the same court

Thumbnail

acquitted five suspected militants who had confessed to taking part in her 2007 assassination.

FULL STORY

NEWS

Controversial Milwaukee Sheriff David Clarke Resigns

Thumbnail

The tough-talking sheriff of Milwaukee County, David Clarke, resigned without explanation Thursday, capping a tumultuous year for the divisive, provocative lawman whose unabashed support for President Donald Trump and in-your-face personality earned him a national following among some conservatives.

FULL STORY

SUBSCRIBE | ABOUT US | ADVERTISE

We respect your right to privacy - view our policy here.

This mailbox is unattended, so please do not reply to this message. Contact us for assistance.

If you no longer wish to receive these emails - unsubscribe here.

This email was sent by: **Forensic Magazine**
100 Enterprise Drive - Suite 600 - Rockaway, NJ 07866-2129

© 2017 Forensic Magazine. All rights reserved.

From: Forensic Magazine
To: Gibney, Alysha (POL)
Subject: ALPR Data Open to Public, California Courts Rule
Date: Friday, September 1, 2017 1:03:16 PM

View this email in your browser.

Forensic News Daily

SEP 01

IN THIS ISSUE

NEWS

Austin Police Partner With UNT Health Science Center

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Crime Alert: chemicals have escaped in your lab

Evidence processing leaves behind a bad smell in your lab. The Halo air filtration system is on the job 24/7 to capture fugitive emissions and return clean air back to the laboratory.

LEARN MORE

FEATURED STORY

ALPR Data Open to Public, California Courts Rule

The automated license plate reader (ALPR) data collected from millions in Los Angeles County is public information, the California Supreme Court ruled this week.

Featured Story

Share

FULL STORY

Ultrafast, Ultra-sensitive GC-MS

Shimadzu's GCMS-QP2020, with the Smart Forensic Database, is the ideal platform for detection and quantitation of targeted drugs in the presence of background interferences.

LEARN MORE

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

Thumbnail

Bodies are piling up at the Houston morgue because of Harvey: Not only did the storm lead to more than 30 deaths, but the widespread flooding has also prevented funeral homes from collecting the corpses of those who died from other causes.

FULL STORY

NEWS

Austin Police Partner With UNT Health Science Center

In the aftermath of its lab's closure, the Austin Police

Thumbnail

Department will now send a majority of its faulty DNA cases to the University of North Texas Health Science Center to determine if retesting must be done.

FULL STORY

Streamlining the Extraction of Drugs Process with Centrifugal Evaporation

Genevac LTD

A method for the extraction of drugs of abuse from urine samples pertaining to drug facilitated sexual assault cases has been developed, involving the use of solid phase extraction techniques prior to screening analysis. Under conventional testing methods, evaporation is achieved using a nitrogen blow down system. This white paper examines the benefits of using a centrifugal evaporation system for drugs of abuse urine sample testing. These benefits include increased sensitivity, reduced cross contamination, and a reduction of time needed to complete the evaporation process.

DOWNLOAD NOW

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Thumbnail

A nurse says she was assaulted and illegally arrested by a Salt Lake City police detective for following a hospital policy that does not allow blood draws from unconscious patients. Footage from University Hospital and officer body cameras shows Detective Jeff Payne and nurse Alex Wubbels in a standoff over whether the policeman should be allowed to get the blood sample.

FULL STORY

NEWS

Pakistan Verdict on Bhutto Assassination Angers Supporters

A Pakistani court on Thursday sentenced two former police officers to 17 years in prison for failing to protect former Prime Minister Benazir Bhutto, but the same court

Thumbnail

acquitted five suspected militants who had confessed to taking part in her 2007 assassination.

FULL STORY

NEWS

Controversial Milwaukee Sheriff David Clarke Resigns

Thumbnail

The tough-talking sheriff of Milwaukee County, David Clarke, resigned without explanation Thursday, capping a tumultuous year for the divisive, provocative lawman whose unabashed support for President Donald Trump and in-your-face personality earned him a national following among some conservatives.

FULL STORY

SUBSCRIBE | ABOUT US | ADVERTISE

We respect your right to privacy - view our policy here.

This mailbox is unattended, so please do not reply to this message. Contact us for assistance.

If you no longer wish to receive these emails - unsubscribe here.

This email was sent by: **Forensic Magazine**
100 Enterprise Drive - Suite 600 - Rockaway, NJ 07866-2129

© 2017 Forensic Magazine. All rights reserved.

From: Forensic Magazine
To: Avery, Lynette (POL)
Subject: ALPR Data Open to Public, California Courts Rule
Date: Friday, September 1, 2017 1:03:10 PM

View this email in your browser.

Forensic News Daily

SEP 01

IN THIS ISSUE

NEWS

Austin Police Partner With UNT Health Science Center

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Crime Alert: chemicals have escaped in your lab

Evidence processing leaves behind a bad smell in your lab. The Halo air filtration system is on the job 24/7 to capture fugitive emissions and return clean air back to the laboratory.

LEARN MORE

FEATURED STORY

ALPR Data Open to Public, California Courts Rule

The automated license plate reader (ALPR) data collected from millions in Los Angeles County is public information, the California Supreme Court ruled this week.

Featured Story

Share

FULL STORY

Ultrafast, Ultra-sensitive GC-MS

Shimadzu's GCMS-QP2020, with the Smart Forensic Database, is the ideal platform for detection and quantitation of targeted drugs in the presence of background interferences.

LEARN MORE

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

Thumbnail

Bodies are piling up at the Houston morgue because of Harvey: Not only did the storm lead to more than 30 deaths, but the widespread flooding has also prevented funeral homes from collecting the corpses of those who died from other causes.

FULL STORY

NEWS

Austin Police Partner With UNT Health Science Center

In the aftermath of its lab's closure, the Austin Police

Thumbnail

Department will now send a majority of its faulty DNA cases to the University of North Texas Health Science Center to determine if retesting must be done.

FULL STORY

Streamlining the Extraction of Drugs Process with Centrifugal Evaporation

Genevac LTD

A method for the extraction of drugs of abuse from urine samples pertaining to drug facilitated sexual assault cases has been developed, involving the use of solid phase extraction techniques prior to screening analysis. Under conventional testing methods, evaporation is achieved using a nitrogen blow down system. This white paper examines the benefits of using a centrifugal evaporation system for drugs of abuse urine sample testing. These benefits include increased sensitivity, reduced cross contamination, and a reduction of time needed to complete the evaporation process.

DOWNLOAD NOW

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Thumbnail

A nurse says she was assaulted and illegally arrested by a Salt Lake City police detective for following a hospital policy that does not allow blood draws from unconscious patients. Footage from University Hospital and officer body cameras shows Detective Jeff Payne and nurse Alex Wubbels in a standoff over whether the policeman should be allowed to get the blood sample.

FULL STORY

NEWS

Pakistan Verdict on Bhutto Assassination Angers Supporters

A Pakistani court on Thursday sentenced two former police officers to 17 years in prison for failing to protect former Prime Minister Benazir Bhutto, but the same court

Thumbnail

acquitted five suspected militants who had confessed to taking part in her 2007 assassination.

FULL STORY

NEWS

Controversial Milwaukee Sheriff David Clarke Resigns

Thumbnail

The tough-talking sheriff of Milwaukee County, David Clarke, resigned without explanation Thursday, capping a tumultuous year for the divisive, provocative lawman whose unabashed support for President Donald Trump and in-your-face personality earned him a national following among some conservatives.

FULL STORY

SUBSCRIBE | ABOUT US | ADVERTISE

We respect your right to privacy - view our policy here.

This mailbox is unattended, so please do not reply to this message. Contact us for assistance.

If you no longer wish to receive these emails - unsubscribe here.

This email was sent by: **Forensic Magazine**
100 Enterprise Drive - Suite 600 - Rockaway, NJ 07866-2129

© 2017 Forensic Magazine. All rights reserved.

From: Forensic Magazine
To: Rabel, Betsy (POL)
Subject: ALPR Data Open to Public, California Courts Rule
Date: Friday, September 1, 2017 1:03:07 PM

View this email in your browser.

Forensic News Daily

SEP 01

IN THIS ISSUE

NEWS

Austin Police Partner With UNT Health Science Center

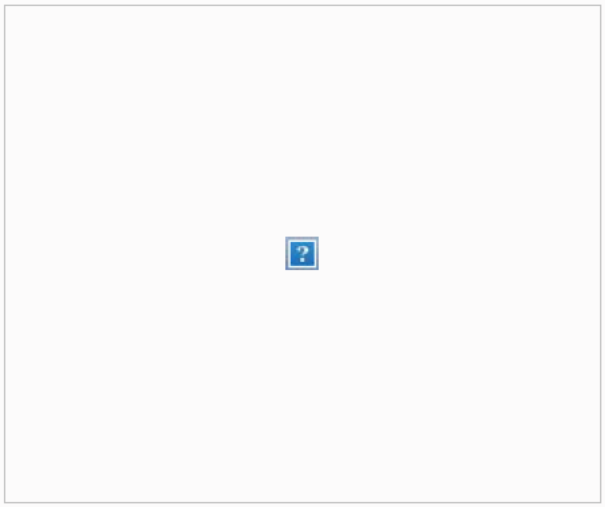
NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Crime Alert: chemicals have escaped in your lab



Evidence processing leaves behind a bad smell in your lab. The Halo air filtration system is on the job 24/7 to capture fugitive emissions and return clean air back to the laboratory.

LEARN MORE

FEATURED STORY

ALPR Data Open to Public, California Courts Rule

The automated license plate reader (ALPR) data collected from millions in Los Angeles County is public information, the California Supreme Court ruled this week.

Featured Story

Share

FULL STORY

Ultrafast, Ultra-sensitive GC-MS

Shimadzu's GCMS-QP2020, with the Smart Forensic Database, is the ideal platform for detection and quantitation of targeted drugs in the presence of background interferences.

LEARN MORE

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

Thumbnail

Bodies are piling up at the Houston morgue because of Harvey: Not only did the storm lead to more than 30 deaths, but the widespread flooding has also prevented funeral homes from collecting the corpses of those who died from other causes.

FULL STORY

NEWS

Austin Police Partner With UNT Health Science Center

In the aftermath of its lab's closure, the Austin Police

Thumbnail

Department will now send a majority of its faulty DNA cases to the University of North Texas Health Science Center to determine if retesting must be done.

FULL STORY

Streamlining the Extraction of Drugs Process with Centrifugal Evaporation

Genevac LTD

A method for the extraction of drugs of abuse from urine samples pertaining to drug facilitated sexual assault cases has been developed, involving the use of solid phase extraction techniques prior to screening analysis. Under conventional testing methods, evaporation is achieved using a nitrogen blow down system. This white paper examines the benefits of using a centrifugal evaporation system for drugs of abuse urine sample testing. These benefits include increased sensitivity, reduced cross contamination, and a reduction of time needed to complete the evaporation process.

DOWNLOAD NOW

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Thumbnail

A nurse says she was assaulted and illegally arrested by a Salt Lake City police detective for following a hospital policy that does not allow blood draws from unconscious patients. Footage from University Hospital and officer body cameras shows Detective Jeff Payne and nurse Alex Wubbels in a standoff over whether the policeman should be allowed to get the blood sample.

FULL STORY

NEWS

Pakistan Verdict on Bhutto Assassination Angers Supporters

A Pakistani court on Thursday sentenced two former police officers to 17 years in prison for failing to protect former Prime Minister Benazir Bhutto, but the same court

Thumbnail

acquitted five suspected militants who had confessed to taking part in her 2007 assassination.

FULL STORY

NEWS

Controversial Milwaukee Sheriff David Clarke Resigns

Thumbnail

The tough-talking sheriff of Milwaukee County, David Clarke, resigned without explanation Thursday, capping a tumultuous year for the divisive, provocative lawman whose unabashed support for President Donald Trump and in-your-face personality earned him a national following among some conservatives.

FULL STORY

SUBSCRIBE | ABOUT US | ADVERTISE

We respect your right to privacy - view our policy here.

This mailbox is unattended, so please do not reply to this message. Contact us for assistance.

If you no longer wish to receive these emails - unsubscribe here.

This email was sent by: **Forensic Magazine**
100 Enterprise Drive - Suite 600 - Rockaway, NJ 07866-2129

© 2017 Forensic Magazine. All rights reserved.

From: Forensic Magazine
To: McDermott, Karen (POL)
Subject: ALPR Data Open to Public, California Courts Rule
Date: Friday, September 1, 2017 1:03:05 PM

View this email in your browser.

Forensic News Daily

SEP 01

IN THIS ISSUE

NEWS

Austin Police Partner With UNT Health Science Center

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Crime Alert: chemicals have escaped in your lab

Evidence processing leaves behind a bad smell in your lab. The Halo air filtration system is on the job 24/7 to capture fugitive emissions and return clean air back to the laboratory.

LEARN MORE

FEATURED STORY

ALPR Data Open to Public, California Courts Rule

The automated license plate reader (ALPR) data collected from millions in Los Angeles County is public information, the California Supreme Court ruled this week.

Featured Story

Share

FULL STORY

Ultrafast, Ultra-sensitive GC-MS

Shimadzu's GCMS-QP2020, with the Smart Forensic Database, is the ideal platform for detection and quantitation of targeted drugs in the presence of background interferences.

LEARN MORE

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

Thumbnail

Bodies are piling up at the Houston morgue because of Harvey: Not only did the storm lead to more than 30 deaths, but the widespread flooding has also prevented funeral homes from collecting the corpses of those who died from other causes.

FULL STORY

NEWS

Austin Police Partner With UNT Health Science Center

In the aftermath of its lab's closure, the Austin Police

Thumbnail

Department will now send a majority of its faulty DNA cases to the University of North Texas Health Science Center to determine if retesting must be done.

FULL STORY

Streamlining the Extraction of Drugs Process with Centrifugal Evaporation

Genevac LTD

A method for the extraction of drugs of abuse from urine samples pertaining to drug facilitated sexual assault cases has been developed, involving the use of solid phase extraction techniques prior to screening analysis. Under conventional testing methods, evaporation is achieved using a nitrogen blow down system. This white paper examines the benefits of using a centrifugal evaporation system for drugs of abuse urine sample testing. These benefits include increased sensitivity, reduced cross contamination, and a reduction of time needed to complete the evaporation process.

DOWNLOAD NOW

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Thumbnail

A nurse says she was assaulted and illegally arrested by a Salt Lake City police detective for following a hospital policy that does not allow blood draws from unconscious patients. Footage from University Hospital and officer body cameras shows Detective Jeff Payne and nurse Alex Wubbels in a standoff over whether the policeman should be allowed to get the blood sample.

FULL STORY

NEWS

Pakistan Verdict on Bhutto Assassination Angers Supporters

A Pakistani court on Thursday sentenced two former police officers to 17 years in prison for failing to protect former Prime Minister Benazir Bhutto, but the same court

Thumbnail

acquitted five suspected militants who had confessed to taking part in her 2007 assassination.

FULL STORY

NEWS

Controversial Milwaukee Sheriff David Clarke Resigns

Thumbnail

The tough-talking sheriff of Milwaukee County, David Clarke, resigned without explanation Thursday, capping a tumultuous year for the divisive, provocative lawman whose unabashed support for President Donald Trump and in-your-face personality earned him a national following among some conservatives.

FULL STORY

SUBSCRIBE | ABOUT US | ADVERTISE

We respect your right to privacy - view our policy here.

This mailbox is unattended, so please do not reply to this message. Contact us for assistance.

If you no longer wish to receive these emails - unsubscribe here.

This email was sent by: **Forensic Magazine**
100 Enterprise Drive - Suite 600 - Rockaway, NJ 07866-2129

© 2017 Forensic Magazine. All rights reserved.

From: Forensic Magazine
To: king, kelley (POL)
Subject: ALPR Data Open to Public, California Courts Rule
Date: Friday, September 1, 2017 1:03:04 PM

View this email in your browser.

Forensic News Daily

SEP 01

IN THIS ISSUE

NEWS

Austin Police Partner With UNT Health Science Center

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Crime Alert: chemicals have escaped in your lab

Evidence processing leaves behind a bad smell in your lab. The Halo air filtration system is on the job 24/7 to capture fugitive emissions and return clean air back to the laboratory.

LEARN MORE

FEATURED STORY

ALPR Data Open to Public, California Courts Rule

The automated license plate reader (ALPR) data collected from millions in Los Angeles County is public information, the California Supreme Court ruled this week.

Featured Story

Share

FULL STORY

Ultrafast, Ultra-sensitive GC-MS

Shimadzu's GCMS-QP2020, with the Smart Forensic Database, is the ideal platform for detection and quantitation of targeted drugs in the presence of background interferences.

LEARN MORE

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

Thumbnail

Bodies are piling up at the Houston morgue because of Harvey: Not only did the storm lead to more than 30 deaths, but the widespread flooding has also prevented funeral homes from collecting the corpses of those who died from other causes.

FULL STORY

NEWS

Austin Police Partner With UNT Health Science Center

In the aftermath of its lab's closure, the Austin Police

Thumbnail

Department will now send a majority of its faulty DNA cases to the University of North Texas Health Science Center to determine if retesting must be done.

FULL STORY

Streamlining the Extraction of Drugs Process with Centrifugal Evaporation

Genevac LTD

A method for the extraction of drugs of abuse from urine samples pertaining to drug facilitated sexual assault cases has been developed, involving the use of solid phase extraction techniques prior to screening analysis. Under conventional testing methods, evaporation is achieved using a nitrogen blow down system. This white paper examines the benefits of using a centrifugal evaporation system for drugs of abuse urine sample testing. These benefits include increased sensitivity, reduced cross contamination, and a reduction of time needed to complete the evaporation process.

DOWNLOAD NOW

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Thumbnail

A nurse says she was assaulted and illegally arrested by a Salt Lake City police detective for following a hospital policy that does not allow blood draws from unconscious patients. Footage from University Hospital and officer body cameras shows Detective Jeff Payne and nurse Alex Wubbels in a standoff over whether the policeman should be allowed to get the blood sample.

FULL STORY

NEWS

Pakistan Verdict on Bhutto Assassination Angers Supporters

A Pakistani court on Thursday sentenced two former police officers to 17 years in prison for failing to protect former Prime Minister Benazir Bhutto, but the same court

Thumbnail

acquitted five suspected militants who had confessed to taking part in her 2007 assassination.

FULL STORY

NEWS

Controversial Milwaukee Sheriff David Clarke Resigns

Thumbnail

The tough-talking sheriff of Milwaukee County, David Clarke, resigned without explanation Thursday, capping a tumultuous year for the divisive, provocative lawman whose unabashed support for President Donald Trump and in-your-face personality earned him a national following among some conservatives.

FULL STORY

SUBSCRIBE | ABOUT US | ADVERTISE

We respect your right to privacy - view our policy here.

This mailbox is unattended, so please do not reply to this message. Contact us for assistance.

If you no longer wish to receive these emails - unsubscribe here.

This email was sent by: **Forensic Magazine**
100 Enterprise Drive - Suite 600 - Rockaway, NJ 07866-2129

© 2017 Forensic Magazine. All rights reserved.

From: Forensic Magazine
To: Murphy, Laurie (POL)
Subject: ALPR Data Open to Public, California Courts Rule
Date: Friday, September 1, 2017 1:02:42 PM

View this email in your browser.

Forensic News Daily

SEP 01

IN THIS ISSUE

NEWS

Austin Police Partner With UNT Health Science Center

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Crime Alert: chemicals have escaped in your lab

Evidence processing leaves behind a bad smell in your lab. The Halo air filtration system is on the job 24/7 to capture fugitive emissions and return clean air back to the laboratory.

LEARN MORE

FEATURED STORY

ALPR Data Open to Public, California Courts Rule

The automated license plate reader (ALPR) data collected from millions in Los Angeles County is public information, the California Supreme Court ruled this week.

Featured Story

Share

FULL STORY

Ultrafast, Ultra-sensitive GC-MS

Shimadzu's GCMS-QP2020, with the Smart Forensic Database, is the ideal platform for detection and quantitation of targeted drugs in the presence of background interferences.

LEARN MORE

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

Thumbnail

Bodies are piling up at the Houston morgue because of Harvey: Not only did the storm lead to more than 30 deaths, but the widespread flooding has also prevented funeral homes from collecting the corpses of those who died from other causes.

FULL STORY

NEWS

Austin Police Partner With UNT Health Science Center

In the aftermath of its lab's closure, the Austin Police

Thumbnail

Department will now send a majority of its faulty DNA cases to the University of North Texas Health Science Center to determine if retesting must be done.

FULL STORY

Streamlining the Extraction of Drugs Process with Centrifugal Evaporation

Genevac LTD

A method for the extraction of drugs of abuse from urine samples pertaining to drug facilitated sexual assault cases has been developed, involving the use of solid phase extraction techniques prior to screening analysis. Under conventional testing methods, evaporation is achieved using a nitrogen blow down system. This white paper examines the benefits of using a centrifugal evaporation system for drugs of abuse urine sample testing. These benefits include increased sensitivity, reduced cross contamination, and a reduction of time needed to complete the evaporation process.

DOWNLOAD NOW

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Thumbnail

A nurse says she was assaulted and illegally arrested by a Salt Lake City police detective for following a hospital policy that does not allow blood draws from unconscious patients. Footage from University Hospital and officer body cameras shows Detective Jeff Payne and nurse Alex Wubbels in a standoff over whether the policeman should be allowed to get the blood sample.

FULL STORY

NEWS

Pakistan Verdict on Bhutto Assassination Angers Supporters

A Pakistani court on Thursday sentenced two former police officers to 17 years in prison for failing to protect former Prime Minister Benazir Bhutto, but the same court

Thumbnail

acquitted five suspected militants who had confessed to taking part in her 2007 assassination.

FULL STORY

NEWS

Controversial Milwaukee Sheriff David Clarke Resigns

Thumbnail

The tough-talking sheriff of Milwaukee County, David Clarke, resigned without explanation Thursday, capping a tumultuous year for the divisive, provocative lawman whose unabashed support for President Donald Trump and in-your-face personality earned him a national following among some conservatives.

FULL STORY

SUBSCRIBE | ABOUT US | ADVERTISE

We respect your right to privacy - view our policy here.

This mailbox is unattended, so please do not reply to this message. Contact us for assistance.

If you no longer wish to receive these emails - unsubscribe here.

This email was sent by: **Forensic Magazine**
100 Enterprise Drive - Suite 600 - Rockaway, NJ 07866-2129

© 2017 Forensic Magazine. All rights reserved.

From: Forensic Magazine
To: Sullivan, Kristen (POL)
Subject: ALPR Data Open to Public, California Courts Rule
Date: Friday, September 1, 2017 1:02:30 PM

View this email in your browser.

Forensic News Daily

SEP 01

IN THIS ISSUE

NEWS

Austin Police Partner With UNT Health Science Center

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Crime Alert: chemicals have escaped in your lab

Evidence processing leaves behind a bad smell in your lab. The Halo air filtration system is on the job 24/7 to capture fugitive emissions and return clean air back to the laboratory.

LEARN MORE

FEATURED STORY

ALPR Data Open to Public, California Courts Rule

The automated license plate reader (ALPR) data collected from millions in Los Angeles County is public information, the California Supreme Court ruled this week.

Featured Story

Share

FULL STORY

Ultrafast, Ultra-sensitive GC-MS

Shimadzu's GCMS-QP2020, with the Smart Forensic Database, is the ideal platform for detection and quantitation of targeted drugs in the presence of background interferences.

LEARN MORE

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

Thumbnail

Bodies are piling up at the Houston morgue because of Harvey: Not only did the storm lead to more than 30 deaths, but the widespread flooding has also prevented funeral homes from collecting the corpses of those who died from other causes.

FULL STORY

NEWS

Austin Police Partner With UNT Health Science Center

In the aftermath of its lab's closure, the Austin Police

Thumbnail

Department will now send a majority of its faulty DNA cases to the University of North Texas Health Science Center to determine if retesting must be done.

FULL STORY

Streamlining the Extraction of Drugs Process with Centrifugal Evaporation

Genevac LTD

A method for the extraction of drugs of abuse from urine samples pertaining to drug facilitated sexual assault cases has been developed, involving the use of solid phase extraction techniques prior to screening analysis. Under conventional testing methods, evaporation is achieved using a nitrogen blow down system. This white paper examines the benefits of using a centrifugal evaporation system for drugs of abuse urine sample testing. These benefits include increased sensitivity, reduced cross contamination, and a reduction of time needed to complete the evaporation process.

DOWNLOAD NOW

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Thumbnail

A nurse says she was assaulted and illegally arrested by a Salt Lake City police detective for following a hospital policy that does not allow blood draws from unconscious patients. Footage from University Hospital and officer body cameras shows Detective Jeff Payne and nurse Alex Wubbels in a standoff over whether the policeman should be allowed to get the blood sample.

FULL STORY

NEWS

Pakistan Verdict on Bhutto Assassination Angers Supporters

A Pakistani court on Thursday sentenced two former police officers to 17 years in prison for failing to protect former Prime Minister Benazir Bhutto, but the same court

Thumbnail

acquitted five suspected militants who had confessed to taking part in her 2007 assassination.

FULL STORY

NEWS

Controversial Milwaukee Sheriff David Clarke Resigns

Thumbnail

The tough-talking sheriff of Milwaukee County, David Clarke, resigned without explanation Thursday, capping a tumultuous year for the divisive, provocative lawman whose unabashed support for President Donald Trump and in-your-face personality earned him a national following among some conservatives.

FULL STORY

SUBSCRIBE | ABOUT US | ADVERTISE

We respect your right to privacy - view our policy here.

This mailbox is unattended, so please do not reply to this message. Contact us for assistance.

If you no longer wish to receive these emails - unsubscribe here.

This email was sent by: **Forensic Magazine**
100 Enterprise Drive - Suite 600 - Rockaway, NJ 07866-2129

© 2017 Forensic Magazine. All rights reserved.

From: Forensic Magazine
To: Conron, John (POL)
Subject: ALPR Data Open to Public, California Courts Rule
Date: Friday, September 1, 2017 1:02:29 PM

View this email in your browser.

Forensic News Daily

SEP 01

IN THIS ISSUE

NEWS

Austin Police Partner With UNT Health Science Center

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Crime Alert: chemicals have escaped in your lab

Evidence processing leaves behind a bad smell in your lab. The Halo air filtration system is on the job 24/7 to capture fugitive emissions and return clean air back to the laboratory.

LEARN MORE

FEATURED STORY

ALPR Data Open to Public, California Courts Rule

The automated license plate reader (ALPR) data collected from millions in Los Angeles County is public information, the California Supreme Court ruled this week.

Featured Story

Share

FULL STORY

Ultrafast, Ultra-sensitive GC-MS

Shimadzu's GCMS-QP2020, with the Smart Forensic Database, is the ideal platform for detection and quantitation of targeted drugs in the presence of background interferences.

LEARN MORE

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

Thumbnail

Bodies are piling up at the Houston morgue because of Harvey: Not only did the storm lead to more than 30 deaths, but the widespread flooding has also prevented funeral homes from collecting the corpses of those who died from other causes.

FULL STORY

NEWS

Austin Police Partner With UNT Health Science Center

In the aftermath of its lab's closure, the Austin Police

Thumbnail

Department will now send a majority of its faulty DNA cases to the University of North Texas Health Science Center to determine if retesting must be done.

FULL STORY

Streamlining the Extraction of Drugs Process with Centrifugal Evaporation

Genevac LTD

A method for the extraction of drugs of abuse from urine samples pertaining to drug facilitated sexual assault cases has been developed, involving the use of solid phase extraction techniques prior to screening analysis. Under conventional testing methods, evaporation is achieved using a nitrogen blow down system. This white paper examines the benefits of using a centrifugal evaporation system for drugs of abuse urine sample testing. These benefits include increased sensitivity, reduced cross contamination, and a reduction of time needed to complete the evaporation process.

DOWNLOAD NOW

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Thumbnail

A nurse says she was assaulted and illegally arrested by a Salt Lake City police detective for following a hospital policy that does not allow blood draws from unconscious patients. Footage from University Hospital and officer body cameras shows Detective Jeff Payne and nurse Alex Wubbels in a standoff over whether the policeman should be allowed to get the blood sample.

FULL STORY

NEWS

Pakistan Verdict on Bhutto Assassination Angers Supporters

A Pakistani court on Thursday sentenced two former police officers to 17 years in prison for failing to protect former Prime Minister Benazir Bhutto, but the same court

Thumbnail

acquitted five suspected militants who had confessed to taking part in her 2007 assassination.

FULL STORY

NEWS

Controversial Milwaukee Sheriff David Clarke Resigns

Thumbnail

The tough-talking sheriff of Milwaukee County, David Clarke, resigned without explanation Thursday, capping a tumultuous year for the divisive, provocative lawman whose unabashed support for President Donald Trump and in-your-face personality earned him a national following among some conservatives.

FULL STORY

SUBSCRIBE | ABOUT US | ADVERTISE

We respect your right to privacy - view our policy here.

This mailbox is unattended, so please do not reply to this message. Contact us for assistance.

If you no longer wish to receive these emails - unsubscribe here.

This email was sent by: **Forensic Magazine**
100 Enterprise Drive - Suite 600 - Rockaway, NJ 07866-2129

© 2017 Forensic Magazine. All rights reserved.

From: Forensic Magazine
To: Bryant, Laura (POL)
Subject: ALPR Data Open to Public, California Courts Rule
Date: Friday, September 1, 2017 1:02:27 PM

View this email in your browser.

Forensic News Daily

SEP 01

IN THIS ISSUE

NEWS

Austin Police Partner With UNT Health Science Center

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Crime Alert: chemicals have escaped in your lab

Evidence processing leaves behind a bad smell in your lab. The Halo air filtration system is on the job 24/7 to capture fugitive emissions and return clean air back to the laboratory.

LEARN MORE

FEATURED STORY

ALPR Data Open to Public, California Courts Rule

The automated license plate reader (ALPR) data collected from millions in Los Angeles County is public information, the California Supreme Court ruled this week.

Featured Story

Share

FULL STORY

Ultrafast, Ultra-sensitive GC-MS

Shimadzu's GCMS-QP2020, with the Smart Forensic Database, is the ideal platform for detection and quantitation of targeted drugs in the presence of background interferences.

LEARN MORE

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

Thumbnail

Bodies are piling up at the Houston morgue because of Harvey: Not only did the storm lead to more than 30 deaths, but the widespread flooding has also prevented funeral homes from collecting the corpses of those who died from other causes.

FULL STORY

NEWS

Austin Police Partner With UNT Health Science Center

In the aftermath of its lab's closure, the Austin Police

Thumbnail

Department will now send a majority of its faulty DNA cases to the University of North Texas Health Science Center to determine if retesting must be done.

FULL STORY

Streamlining the Extraction of Drugs Process with Centrifugal Evaporation

Genevac LTD

A method for the extraction of drugs of abuse from urine samples pertaining to drug facilitated sexual assault cases has been developed, involving the use of solid phase extraction techniques prior to screening analysis. Under conventional testing methods, evaporation is achieved using a nitrogen blow down system. This white paper examines the benefits of using a centrifugal evaporation system for drugs of abuse urine sample testing. These benefits include increased sensitivity, reduced cross contamination, and a reduction of time needed to complete the evaporation process.

DOWNLOAD NOW

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Thumbnail

A nurse says she was assaulted and illegally arrested by a Salt Lake City police detective for following a hospital policy that does not allow blood draws from unconscious patients. Footage from University Hospital and officer body cameras shows Detective Jeff Payne and nurse Alex Wubbels in a standoff over whether the policeman should be allowed to get the blood sample.

FULL STORY

NEWS

Pakistan Verdict on Bhutto Assassination Angers Supporters

A Pakistani court on Thursday sentenced two former police officers to 17 years in prison for failing to protect former Prime Minister Benazir Bhutto, but the same court

Thumbnail

acquitted five suspected militants who had confessed to taking part in her 2007 assassination.

FULL STORY

NEWS

Controversial Milwaukee Sheriff David Clarke Resigns

Thumbnail

The tough-talking sheriff of Milwaukee County, David Clarke, resigned without explanation Thursday, capping a tumultuous year for the divisive, provocative lawman whose unabashed support for President Donald Trump and in-your-face personality earned him a national following among some conservatives.

FULL STORY

SUBSCRIBE | ABOUT US | ADVERTISE

We respect your right to privacy - view our policy here.

This mailbox is unattended, so please do not reply to this message. Contact us for assistance.

If you no longer wish to receive these emails - unsubscribe here.

This email was sent by: **Forensic Magazine**
100 Enterprise Drive - Suite 600 - Rockaway, NJ 07866-2129

© 2017 Forensic Magazine. All rights reserved.

From: Forensic Magazine
To: Oley, Carl (POL)
Subject: ALPR Data Open to Public, California Courts Rule
Date: Friday, September 1, 2017 1:02:12 PM

View this email in your browser.

Forensic News Daily

SEP 01

IN THIS ISSUE

NEWS

Austin Police Partner With UNT Health Science Center

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Crime Alert: chemicals have escaped in your lab

Evidence processing leaves behind a bad smell in your lab. The Halo air filtration system is on the job 24/7 to capture fugitive emissions and return clean air back to the laboratory.

LEARN MORE

FEATURED STORY

ALPR Data Open to Public, California Courts Rule

The automated license plate reader (ALPR) data collected from millions in Los Angeles County is public information, the California Supreme Court ruled this week.

Featured Story

Share

FULL STORY

Ultrafast, Ultra-sensitive GC-MS

Shimadzu's GCMS-QP2020, with the Smart Forensic Database, is the ideal platform for detection and quantitation of targeted drugs in the presence of background interferences.

LEARN MORE

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

Thumbnail

Bodies are piling up at the Houston morgue because of Harvey: Not only did the storm lead to more than 30 deaths, but the widespread flooding has also prevented funeral homes from collecting the corpses of those who died from other causes.

FULL STORY

NEWS

Austin Police Partner With UNT Health Science Center

In the aftermath of its lab's closure, the Austin Police

Thumbnail

Department will now send a majority of its faulty DNA cases to the University of North Texas Health Science Center to determine if retesting must be done.

FULL STORY

Streamlining the Extraction of Drugs Process with Centrifugal Evaporation

Genevac LTD

A method for the extraction of drugs of abuse from urine samples pertaining to drug facilitated sexual assault cases has been developed, involving the use of solid phase extraction techniques prior to screening analysis. Under conventional testing methods, evaporation is achieved using a nitrogen blow down system. This white paper examines the benefits of using a centrifugal evaporation system for drugs of abuse urine sample testing. These benefits include increased sensitivity, reduced cross contamination, and a reduction of time needed to complete the evaporation process.

DOWNLOAD NOW

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Thumbnail

A nurse says she was assaulted and illegally arrested by a Salt Lake City police detective for following a hospital policy that does not allow blood draws from unconscious patients. Footage from University Hospital and officer body cameras shows Detective Jeff Payne and nurse Alex Wubbels in a standoff over whether the policeman should be allowed to get the blood sample.

FULL STORY

NEWS

Pakistan Verdict on Bhutto Assassination Angers Supporters

A Pakistani court on Thursday sentenced two former police officers to 17 years in prison for failing to protect former Prime Minister Benazir Bhutto, but the same court

Thumbnail

acquitted five suspected militants who had confessed to taking part in her 2007 assassination.

FULL STORY

NEWS

Controversial Milwaukee Sheriff David Clarke Resigns

Thumbnail

The tough-talking sheriff of Milwaukee County, David Clarke, resigned without explanation Thursday, capping a tumultuous year for the divisive, provocative lawman whose unabashed support for President Donald Trump and in-your-face personality earned him a national following among some conservatives.

FULL STORY

SUBSCRIBE | ABOUT US | ADVERTISE

We respect your right to privacy - view our policy here.

This mailbox is unattended, so please do not reply to this message. Contact us for assistance.

If you no longer wish to receive these emails - unsubscribe here.

This email was sent by: **Forensic Magazine**
100 Enterprise Drive - Suite 600 - Rockaway, NJ 07866-2129

© 2017 Forensic Magazine. All rights reserved.

From: Forensic Magazine
To: Mir, Anum (POL)
Subject: ALPR Data Open to Public, California Courts Rule
Date: Friday, September 1, 2017 1:04:33 PM

View this email in your browser.

Forensic News Daily

SEP 01

IN THIS ISSUE

NEWS

Austin Police Partner With UNT Health Science Center

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Crime Alert: chemicals have escaped in your lab

Evidence processing leaves behind a bad smell in your lab. The Halo air filtration system is on the job 24/7 to capture fugitive emissions and return clean air back to the laboratory.

LEARN MORE

FEATURED STORY

ALPR Data Open to Public, California Courts Rule

The automated license plate reader (ALPR) data collected from millions in Los Angeles County is public information, the California Supreme Court ruled this week.

Featured Story

Share

FULL STORY

Ultrafast, Ultra-sensitive GC-MS

Shimadzu's GCMS-QP2020, with the Smart Forensic Database, is the ideal platform for detection and quantitation of targeted drugs in the presence of background interferences.

LEARN MORE

NEWS

Harvey Deaths, Other Fatalities Push Morgue to Near Capacity

Thumbnail

Bodies are piling up at the Houston morgue because of Harvey: Not only did the storm lead to more than 30 deaths, but the widespread flooding has also prevented funeral homes from collecting the corpses of those who died from other causes.

FULL STORY

NEWS

Austin Police Partner With UNT Health Science Center

In the aftermath of its lab's closure, the Austin Police

Thumbnail

Department will now send a majority of its faulty DNA cases to the University of North Texas Health Science Center to determine if retesting must be done.

FULL STORY

Streamlining the Extraction of Drugs Process with Centrifugal Evaporation

Genevac LTD

A method for the extraction of drugs of abuse from urine samples pertaining to drug facilitated sexual assault cases has been developed, involving the use of solid phase extraction techniques prior to screening analysis. Under conventional testing methods, evaporation is achieved using a nitrogen blow down system. This white paper examines the benefits of using a centrifugal evaporation system for drugs of abuse urine sample testing. These benefits include increased sensitivity, reduced cross contamination, and a reduction of time needed to complete the evaporation process.

DOWNLOAD NOW

NEWS

Video Shows Utah Nurse Screaming, Being Dragged Into Police Car After Refusing to Let Officer Take Blood from Unconscious Victim

Thumbnail

A nurse says she was assaulted and illegally arrested by a Salt Lake City police detective for following a hospital policy that does not allow blood draws from unconscious patients. Footage from University Hospital and officer body cameras shows Detective Jeff Payne and nurse Alex Wubbels in a standoff over whether the policeman should be allowed to get the blood sample.

FULL STORY

NEWS

Pakistan Verdict on Bhutto Assassination Angers Supporters

A Pakistani court on Thursday sentenced two former police officers to 17 years in prison for failing to protect former Prime Minister Benazir Bhutto, but the same court

Thumbnail

acquitted five suspected militants who had confessed to taking part in her 2007 assassination.

FULL STORY

NEWS

Controversial Milwaukee Sheriff David Clarke Resigns

Thumbnail

The tough-talking sheriff of Milwaukee County, David Clarke, resigned without explanation Thursday, capping a tumultuous year for the divisive, provocative lawman whose unabashed support for President Donald Trump and in-your-face personality earned him a national following among some conservatives.

FULL STORY

SUBSCRIBE | ABOUT US | ADVERTISE

We respect your right to privacy - view our policy here.

This mailbox is unattended, so please do not reply to this message. Contact us for assistance.

If you no longer wish to receive these emails - unsubscribe here.

This email was sent by: **Forensic Magazine**
100 Enterprise Drive - Suite 600 - Rockaway, NJ 07866-2129

© 2017 Forensic Magazine. All rights reserved.

From: Kristopher Wright
To: Egnitz, Brian (POL)
Cc: John Tedona
Subject: ALPR Fixed Camera Quote
Date: Friday, March 24, 2017 1:57:46 PM
Attachments: MHQ Quote per Contract #SP16-MSPVEH-F80.pdf
MSP DIRECT_P492 Fixed Camera + Plate Alert Software.pdf
Plate Alert brochure.pdf

Brian,

Please see attached pricing as per our recent phone discussion.

Let me know contact me if you need anything further.

Thank you,

Kristopher Wright
Public Safety Team - Account Manager
401 Elm St., Marlborough, MA 01752
p. 508-573-2618 | c. 603-325-0995
kwright@mhq.com | www.mhq.com | Facebook

From: Egnitz, Brian (POL)
To: Mason, Christopher (POL)
Cc: Quinn, Dermot (POL)
Subject: ALPR Quote
Date: Friday, March 24, 2017 2:14:02 PM
Attachments: Est_QACS172053_from_Access_Control_Systems_7204.pdf
DELLR730_APP_30000007937101.pdf
DELLR730_DB_30000007929391.pdf
MSP DIRECT_P492 Fixed Camera + Plate Alert Software.pdf
Plate Alert brochure.pdf
MHQ Quote per Contract #SP16-MSPVEH-F80 - Rev 1.pdf

Please find the attached quotes for 30 LPRs and 30 Solar Trailers. I'm still waiting on a quote for 2 4x4 trucks.

Total LPR $419,610
Total Trailer $508,400.00
Server Upgrade $29,365.77
Total Cost $957,357.77 + 2 4x4 trucks $ TBD

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
978-451-3710 (Maynard)
508-988-7216 (GHQ)

From: Comeau, Melissa (POL)
To: Tapis, Stephen C (POL)
Subject: ALPRs
Date: Thursday, May 4, 2017 11:13:00 AM
Attachments: 3Camera-Fitzgerald (3).docx

This is the most recent quote I found @ $20,320 each. I would assume it's increased to at least $23,000-$25,000 now since that was 4 years ago.

Melissa Comeau
Fiscal Officer V: Receivables Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2137
Melissa.comeau@massmail.state.ma.us

From: Fitzgerald, Thomas (POL)
Sent: Tuesday, October 29, 2013 6:42 PM
To: Comeau, Melissa (POL)
Subject: FW: Revised

Can I have a PO for the PRISM grant please.

We are a little over can we cover with UCR?

From: Clay Chase [mailto:cchase@imperialmunicipal.com]
Sent: Tuesday, October 29, 2013 6:34 PM
To: Fitzgerald, Thomas (POL)
Subject: Revised

Lt. Fitzgerald,

See attached, let me know if this looks the way you need it.

Clay Chase
President
cchase@imperialmunicipal.com
Ph: **508-422-1000**
Fax: **508-634-9808**



From: Comeau, Melissa (POL)
To: Tapis, Stephen C (POL)
Subject: ALPRs
Date: Thursday, May 4, 2017 11:13:57 AM
Attachments: 3Camera-Fitzgerald (3).docx

This is the most recent quote I found @ $20,320 each. I would assume it's increased to at least $23,000-$25,000 now since that was 4 years ago.

Melissa Comeau
Fiscal Officer V: Receivables Manager
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2137
Melissa.comeau@massmail.state.ma.us

From: Fitzgerald, Thomas (POL)
Sent: Tuesday, October 29, 2013 6:42 PM
To: Comeau, Melissa (POL)
Subject: FW: Revised

Can I have a PO for the PRISM grant please.

We are a little over can we cover with UCR?

From: Clay Chase [mailto:cchase@imperialmunicipal.com]
Sent: Tuesday, October 29, 2013 6:34 PM
To: Fitzgerald, Thomas (POL)
Subject: Revised

Lt. Fitzgerald,

See attached, let me know if this looks the way you need it.

Clay Chase
President
cchase@imperialmunicipal.com
Ph: **508-422-1000**
Fax: **508-634-9808**



From: Egnitz, Brian (POL)
To: Quinn, Dermot (POL); Mason, Christopher (POL)
Subject: April 7
Date: Thursday, March 23, 2017 11:10:53 AM
Attachments: SharePointFieldPropBK.pptx

Hi LTC.,

Does April 7th work to host Field Services and discuss the Fusion Core Project (see rough draft attached)?

-Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
978-451-3710 (Maynard)
508-988-7216 (GHQ)

From: Upton, Paul (POL)

Bcc: Cogan, James; emcgovern@agawam.ma.us; William Scholtz; clsullivan@amherst.edu; Higginbottam, Mark; smathias@aquinnahpolice.us; Michael Sheehan; Diane Wilder; Burman, Ed; Carl, Steven B; ke.leonard@assumption.edu; st.bodogh@assumption.edu; jrogers@attleboropolice.org; scott.mills@auburnmasspolice.org; Ehauvuy@avonmass.org; bgill@ayer.ma.us; jpollard@babson.edu; krichardson@babson.edu; mellynm@barnstablepolice.com; richard.menard@becker.edu; Jones, Scott; mbeaupre@belchertown.org; nlozier@belchertown.org; pgarabedian@belmontpd.org; O"Leary, Brendan; Bentley PD, limbracsio; LeLacheur, John G.; Loether, Travis; Flaherty, David; tgiannop@bu.edu; besip@townofbourne.com; wobrien@boxborough-ma.gov; jmolloy@braintreema.gov; kelley@brandeis.edu; pjudge@brewster-ma.gov; Lacy, Keith; pcullinane@brooklinema.gov; Tigges, James; Mills, Glen; sdemarco@cambridgepolice.org; tkeleher@town.canton.ma.us; kahern@capecod.edu; Wood, Gary; manderson@chathampolicema.com; Spinney, James; Roark, John; rgriffin@chelseama.gov; mcosta@chicopeepolice.com; mwilk@chicopeepolice.com; pmorrison@concordma.gov; Goldman, B; Morahan, Jow; Ouimette, Kenneth; sslavin@danversma.gov; dkenney@dartmouthpd.org; Buckley, Michel; asokoloski@police.deerfield.ma.us; pbenson@town.dennis.ma.us; amclaughlin@douglasma.org; weagles@dovermapd.com; McGowan, Peter; Dow, James; Downes, James G. III; kroderick@eastham-ma.gov; Kulhawik, Edward; dscribner@easthampton.org; calexander@easthampton.org; Cdolby@edgartown-ma.us; cfemino@endicott.edu; jerickson@endicott.edu; Blair, Christopher; Davis, Ryan; melissa.trzepacz@cityofeverett.org; Cabral, Joseph P.; tmauretti@frpd.org; Dunne, Edward A.; christian.anthony@hq.dhs.gov; dcrafts@fisher.edu; sgiannini@police.fitchburgma.gov; cboucha5@fitchburgstate.edu; Brickman, Donald; Hannon, John; Medeiros, Brad; mmanocchio@franklinpolice.com; ldrake@franklinpolice.com; Emcavene@gardner-ma.gov; Cudmore, Donald; Liam O"Rourke; Cullen, Jim; Gillen, Jeffery; Kuc Jr, Mitchell; tbroderick@police.halifax.ma.us; aneill@hamiltonma.gov; Miksch, Michael; Denmark, Edward D.; David Burns; Martin Fay; brackett@harwichpolice.com; Pistone, Bob; oshear@hingham-ma.gov; Smith, William; Haughey, Bryan C.; Todd, Charles; det.sevigne@holyokepd.org; Sgtmahan@hopedale-ma.gov; dshane@hopkintonpd.org; Shea, Chris; jhubbard@ipswichpolice.org; tkelley@kpdmass.org; sburdick@town.lee.ma.us; Sheehan, Timothy; jbarry@lexingtonma.gov; McLean, Mike; Kennedy, Sean; RSmith@lowellma.gov; Tulik, Louis; mluth@lunenburgonline.com; scannell@lynnpolice.org; Freeman, Matthew; tnaze@marlborough-ma.gov; ssullivan@mashpeepd.com; dfarley@massart.edu; George Sherrill; tdmahoney@partners.org; kbolognese@partners.org; mbiedenbach@mgh.harvard.edu; Pierce, Al; Rivers, Kim; Cleblanc@mattapoisettpolice.com; Seeley, Rich; Pappalardo, Mike; chief.landry@millvillepolice.com; jhoffman@montague.net; m_croteau@mecc.mass.edu; j_halkola@mwcc.mass.edu; Furlong, Tim; tclinger@police.nantucket-ma.gov; Grassey, Brian; Schlittler, Mike; Roberto.Dacunha@newbedfordpd.com; michael.ryan@nemusic.edu; msugrue@newburyportpolice.com; Fontano, Steve; Jack Caulfield; heinz@virtualnorfolk.org; dcronin@napd.us; jdirenzo@nattleboro.com; 305@nbpolice.net; dhowe@nrpd.org; Cook, David; aborowski@northamptonma.gov; wlyver@town.northborough.ma.us; tlabrie@northbridgemass.org; r.coppa@neu.edu; w.lynch@northeastern.edu; R.janusz@northeastern.edu; Leighton, Robert F.; Petersen, Thomas; ddooley@norwellpolice.com; dwennerstrand@norwoodma.gov; jgover@norwoodma.gov; william.murdock@oakham-ma.gov; Higgins, Kevin; wmarcelonis@town.oxford.ma.us; p.lukaskiewicz@palmerpolice.org; Maskalenko, Tom; asteben@pittsfieldpd.org; Mark Trapani; Souza, Paul; ltgomes@plymouthpolice.com; bcranshaw@plymptonpd.org; steri@plymptonpd.org; Dillon, Patrick S.; Golden, Jim; Monteith, Bill; Holmes, Derek; Ramos, Brian; dkemmett@townofrochester.com; mschmink@pd.rockportma.gov; r.adams@rowleypolice.com; tmccauley@rutlandpd.us; bradley.goodhale@vermont.gov; rriggs@salemstate.edu; sturcott@salemstate.edu; Kforget@salisburypolice.com; tmurphy@townofsandwich.net; fmorello@saguspd.com; okirkbride@scituatepolice.org; enod@seekonkpd.com; jmccarthy@pd.shrewsburyma.gov; mcappucci@pd.shrewsburyma.gov; Finacom, Timothy; bthibodeau@pd.shrewsburyma.gov; mmcginnis@pd.shrewsburyma.gov; pbrown@pd.shrewsburyma.gov; g_neto@somersetpd.org; j_matos@somersetpd.org; Cabral, Mike; sowaw@southhadleypolice.org; McCarthy, Sean; Murray, Jim; hcollete@spencerpolice.org; esdejong@stcc.edu; Johnson, D; scarroll@stoneham-ma.gov; dbamford@stonehill.edu; Carnes, Peter L.; Obuchowski, Ronald; shurlingjr@sudbury.ma.us; jconnolly2@suffolk.edu; d.perry@suttonpolice.com; Cassidy, Timothey; Ryan, Gregory; Walsh, Edward J.; Columbus, Ryan; dmazza@townsendpd.org; danziger@truropolice.org; Tilton, Joseph; Wagner, Shaun; archbald@umass.edu; ted.carlson2@umassmemorial.org; john.luippold@umassmed.edu; brivard@uptonma.gov; patrick.m.brown@uscg.mil; sprior@uxbridge-ma.gov; Tburke@uxbridge-ma.gov; Smith, Rick; ksilva@wakefieldpd.org; DiNanno, Rich; rkelleher@walpolepd.com; Maher, Tim; Smith, Brian; slawrence@townofware.com; joconnor@police.watertown-ma.gov; Cunningham, Wayne; geraldine.lapense@wellfleet-ma.gov; Gray, Jonathan; Jcraven@wbpd.com; mmincone@wt-pd.com; pgoodney@town.westborough.ma.us; ddonohue@wne.edu; mfoyle@westfield.ma.edu; scoughlin@westfield.ma.edu; dconnell@westfordma.gov; Rleblanc@westminster-ma.gov; kelly.t@westonmass.org; LtBell@westport-ma.gov; rregan@weymouth.ma.us; dgalvin@weymouth.ma.us; santiago_christopher@wheatoncollege.edu; mpoirier@whitman-ma.gov; swilliam@williamstown.net; Pupa, Brian; dmacauley@winchesterpd.org; O"Connell, Dan; jgoodwin@town.winthrop.ma.us; Antul, Tiana Marie; Flemming, Sean; Wattst@worcesterma.gov; cpcarpen@wpi.edu; bgreen@wpi.edu; wmcgrath@police.wrentham.ma.us; Schneeweis, David; darrell.richardson@jud.state.ma.us; thomas.connolly@jud.state.ma.us; Cooke, Peter (POL); John.Moran2@state.ma.us; james.w.smith@state.ma.us; Ferrari, Michael (POL); Clements Jr, Robert F (POL); Mahoney, Richard (POL); Barton, Shannan (POL); michael.barry@atf.gov

Subject: Automated License Plate Reader survey; response requested

Date: Tuesday, June 20, 2017 11:14:00 AM

Attention all Liaison Officers

Earlier today, all Police Chiefs were sent a link to a survey which the Commonwealth Fusion Center is presently conducting.

The **Commonwealth Fusion Center** is compiling current data on the status of Automated License Plate Readers (ALPR) that are in use across the Commonwealth. We are requesting you or a designated person in your agency to please answer the applicable questions in the survey at your earliest convenience. Even if your agency does not currently have or use ALPRs, we would appreciate your response.

The survey can be found using the following link: https://www.surveymonkey.com/r/S3HFB7V

If you have already received this email from the Chiefs email distribution, I apologize for the duplicate request. If you have any questions, please feel free to contact me. Your cooperation is greatly appreciated.

Paul J. Upton
Training Coordinator
Massachusetts State Police
Commonwealth Fusion Center
124 Acton St.
Maynard, MA 01754
978-451-3724

From: Mason, Christopher (POL)
To: Hughes, Francis P (POL)
Cc: Quinn, Dermot (POL)
Subject: CFC ALPR Program Overview
Date: Wednesday, May 31, 2017 11:12:00 AM
Attachments: CFC ALPR Program Overview.docx.doc
ALPR DCJIS Policy - Final 20131008.pdf
LPR MOU V2.doc
IACP License Plate Readers Policy.pdf
SOC-11 Automatic License Plate Recognition.doc

Sir,

Please find attached a To:From which provides an overview of the Commonwealth Fusion Center's Automated License Plate Reader (ALPR) Program and addresses the questions you posed in a previous email. Should you require any additional information, please advise. Thank you.

Major Christopher S. Mason, #2401
Division of Investigative Services
Massachusetts State Police
Commonwealth Fusion Center

From: Mason, Christopher (POL)
To: Egnitz, Brian (POL); Griffin, Daniel (POL)
Subject: CFC ALPR Program Overview.docx
Date: Wednesday, May 31, 2017 6:19:00 AM
Attachments: CFC ALPR Program Overview.docx.doc
ALPR DCJIS Policy - Final 20131008.pdf
LPR MOU V2.doc
IACP License Plate Readers Policy.pdf
SOC-11 Automatic License Plate Recognition.doc

Sirs,

The D/S tasked me with providing him an overview of the CFC ALPR program.(current and proposed ALPR assets, retention time, hotlist creation and notification, database location and contribution, etc.) Please see the attached CFC Overview doc. If you could do a quick read through and provide any corrections or feedback , I would appreciate it. I have a high noon deadline today for submission.

Dan, Do you have numbers on how many ALPR cameras DFS has out on the road. If so, I can add that.

Sorry for the short turnaround time. Thanks again.

Major Christopher S. Mason, #2401
Division of Investigative Services
Massachusetts State Police
Commonwealth Fusion Center

From:	SLTT Partner Engagement
To:	RISS Center; Fusion Center Directors; HIDTA Directors; HIDTA ISC Managers; SLIC; SL Partners
Cc:	Field Ops (ALL); OSLLE; DHS.IGA
Subject:	CICC Release of the License Plate Reader (LPR) Policy Development Template for Use in Intelligence and Investigative Activities
Date:	Wednesday, February 8, 2017 8:36:23 AM
Attachments:	LPR Policy Template FINAL 2-7-17.pdf

Partners–

Through a collaborative partnership among the associations represented on the Criminal Intelligence Coordinating Council (CICC), the U.S. Department of Homeland Security, the Bureau of Justice Assistance, and numerous federal, state, and local partners, we are pleased to announce the official release of the ***License Plate Reader Policy Development Template for Use in Intelligence and Investigative Activities*** (LPR Policy Template). This policy guidance resource is designed specifically for law enforcement entities and fusion centers to assist their efforts developing and implementing comprehensive privacy, civil rights, and civil liberties policies regarding the use of automated license plate readers (ALPRs or LPRs) in intelligence and investigative activities. Justice entities are turning to LPR technology to help solve crimes, recover abducted children, detect trafficking rings, and support terrorism investigations. However, when considering or implementing an LPR program, individual privacy, civil rights, and civil liberties must also be vigorously protected. Justice entities should therefore develop appropriate policies and procedures to guard against possible errors and other potential problems. Such proactive work supports and enhances the justice entity's ability to fulfill its mission while also protecting the privacy, civil rights, and civil liberties of community members. Through the effective and responsible use of LPR technology, agencies strengthen trust and public confidence.

Developed by state, local, and federal law enforcement practitioners with LPR expertise and privacy subject-matter experts (SMEs), the provisions of the LPR Policy Template are intended to be incorporated into agency operational policies and day-to-day operations. Each section represents a fundamental component of a comprehensive policy that includes baseline provisions on LPR information collection; information quality; access and disclosure; redress; security, retention, and destruction; accountability and enforcement; and training. Sample language is provided for each recommended provision, as well as appendices that contain a glossary of terms and definitions, citations to federal and case law, and a draft model policy.

Please also distribute this to your association and organization members.

Thank you,

Mr. Vernon Keenan
Chair, Criminal Intelligence Coordinating Council

Director, Georgia Bureau of Investigation

Deputy Chief Mike Downing
Vice-chair, Criminal Intelligence Coordinating Council
Los Angeles Police Department

From: CJIS GROUP Newsletter
To: McCarthy, Steven (POL)
Subject: CJIS GROUP Newsletter | MAY 01, 2017
Date: Monday, May 1, 2017 10:10:47 AM

Click here to view this message in a browser window.





SLED TrendZ | MAY 01, 2017

Meeting Citizen Expectations, Bridging the Gap Between Public and Private Sector

Click here to register FREE

NEWS & VIEWS

- Corrections Agency Scraps Prison Health Contract
- Want a Rhode Island Driver's License? Smiling No Longer Allowed
- Gunfire Sensors Credited With Quick Arrest in Fresno Rampage
- Maryland MVA Driving Test App Receives Prestigious International Interactive Media Award
- Tyler Technologies Signs $20 Million Agreement with the New York State Department of Taxation and Finance and the Office of Information Technology Services
- Chicago To Replace Computer-Automated Dispatch System
- Washington Township Continues Fire Department System Upgrade
- Newark Police to Get Dash Cams, Body Cams In Pilot Program
- GeoComm Publishes Case Study Highlighting the State of Iowa's Path to GIS Data Readiness for NG9-1-1
- Sheriff's Office Gets New Software
- Lafayette Taps IoT for Air Quality Data
- Tyler Technologies (TYL) Announces $36M Agreement with Cook County, Illinois for Odyssey Solution
- Feasibility Study For Johnson City, TN
- State CIOs Look To Agile
- Tyre Residents Surveyed On Desire For Broadband Access
- Ports Of Lewiston And Clarkston Finally Correct Conduit Conundrum
- How Atlanta Manages Its New Traffic Headache

RELATED NEWS

- FirstNet Holds International Forum
- Emergency workers optimistic about FirstNet technology
- FirstNet Weekly Update to the Public Safety Advisory Committee (PSAC) – April 17, 2017
- Montana aims to

- Editorial: Grand Island Is Right To Explore Its Own Internet Service
- BVU OptiNet Update: Deal Coming Together
- Monroe County, Pa., Issues RFP For 'Monroe Gigabit Project'
- How To Cut Data Center Energy Use
- Digital SouthWest Videos Now Available
- IoT Is The Glue Holding Our Smart Cities Together
- GSA Launches Virtual Assistant Pilot
- DHS Preps Cyber Incident Data Repository
- How One City's 'Not Afraid To Fail" Attitude Is Making It Smarter
- Challenge Grant Update: How Austin Is Getting Smart About Equality
- Facebook Says Citywide Wireless Internet For San Jose Is 'Around The Corner'
- SD Inching Closer To Being First In Nation To Have State 911 System
- For Local Governments, Better Websites Remain Key To Citizen Engagement
- Police Body Cameras Would Be Useful, But Expensive To Implement
- Marquette University Establishes Milwaukee Area's First Cyber Security Center
- New Computer-Aided Dispatch System Unites Local Public Safety Agencies
- Greenville Police To Wear Body Cameras By The First Week Of May
- Scott County to pay more for software
- Getting Power To The Grid After A Cyber Attack
- Archiving Tips For Public Sector Agencies
- Kinston Police Start New Initiative To Catch Suspects On Camera
- County, E911 Working On $3M Radio And Infrastructure Project
- Law Enforcement Utilizing Crowdsourcing Tech To Fight Child Pornography
- Tablets Let Inmates Go Online At Polk County Jail
- Iowa State Police Department Uses Twitter Like Another Tool On Its Belt

Not Enough Time To Respond To RFP'S?

Click Here to Beat the Deadline!

join FirstNet emergency network

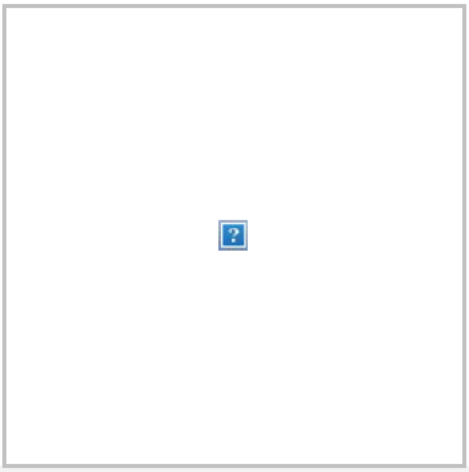
- FirstNet's Nationwide Network: A promising opportunity for community paramedicine programs
- PSAC Profile: National Emergency Number Association (NENA)
- Journey to FirstNet a story of remarkable persistence, refusal to succumb to doubters

DISCIPLINE SPECIFIC RESOURCES

- FirstNet and Law Enforcement
- FirstNet and Fire Services
- FirstNet and Emergency Medical Services
- FirstNet and Emergency Management

Developing Opportunities

The Drawing Board: Here are some of the newly discovered IT initiatives being planned in agencies nationwide:



Status: PRE-RFP

The **Caddo Parish 9-1-1**, on behalf of the Caddo Parish Sheriff Office, Shreveport Police Department, Shreveport Fire Department, Caddo Parish Fire Districts, Vivian Police Department, Greenwood Police Department, Blanchard Police Department, Oil City Police Department, Mooringsport Police Department, Rodessa Police Department, Gilliam Police Department, Ida Police Department, Hosston Police Department, North Caddo Medical Center, Balentine Ambulance and Life Air Rescue, will acquire a parish-wide **P25 Radio System upgrade** **(Estimated Cost: $10M-$25M)** .....Click for opportunity details

Status: PRE-RFP

The **Los Angeles County Metropolitan Transportation Authority (LA METRO)** will complete a **Metro Red Line Access Control Replacement**. The project will consist of replacing the existing 25 year old HID proxcard system with a new Sielox access control system **(Estimated Cost: $2-$5M)** .....Click for opportunity details

Status: PROBABLE CONTRACT NEGOTIATIONS

The **Texas Office of Court Administration (OCA)**, in conjunction with the Texas Department of Transportation Texas, is planning to implement a **Statewide Electronic Citation System**. OCA is exploring the potential means and cost of developing, implementing and operating a Statewide Electronic Citation System to capture electronic and paper citations from participating jurisdictions.....Click for opportunity details

Status: PRE-RFQ WATCH LIST

The **Pennsylvania Department of Transportation (PennDOT)** has determined the need for a new **Modernized Vehicle Driver License System ("MVDLS")**. PennDOT intends to modernize Driver and Vehicle Services systems built on technologies that have become outdated.....Click for opportunity details

Not enough time to respond to RFP's?

Click here to Beat the Deadline

Industry News

- Motorola Solutions and RapidSOS Introduce Precise Location for 9-1-1 Smartphone Calls
- Hyland Software is said to be closing in on a giant purchase
- AvePoint Launches Office 365 Migration and Management Software Donation Program for Not-for-Profit Organizations through TechSoup
- Wireless Tech Comes of Age for More Networks

- Schneider Electric Canada Selects Datalliance as Platform for Vendor Managed Inventory (VMI)
- IBM Opens Four New Cloud Data Centers in the United States to Support Growing Demand for Cognitive Capabilities
- 3M Improves Mobile ALPR with Processor SX4 (Learn More, Video)
- Distributed analytics meets distributed data
- NCS4 Completes Formal Lab Testing On Passport Systems Smartshield System For Venue Security
- Mediware Takes Leadership Position for CPR+ and CareTend Software in Specialty Pharmacy Research Study
- Fujitsu-GlobeRanger and Switlik collaborate to use IoT technology to enhance aviation safety
- SunGard Public Sector is Now Superion
- **Windstream Redefines Continuity for the Cloud**
- New Report Cites Sungard Availability Services Among Leaders in Disaster Recovery as a Service
- Schneider Electric Helps Missouri Cities Improve Public Works Operations With Advanced Metering
- Aware Introduces Indigo|Onboard™, A Cloud-Based Biometric Identity Solution For Better Onboarding
- Cumberland County CommuniCare Bills in Real-Time With AlphaFlex EHR Software
- Minneapolis-based Premium Waters selects OneNeck to manage their IT solution
- New PCTEL MIMO Yagi Antenna Supports SCADA Networks on Licensed 700 MHz Spectrum
- Crossmatch to reveal the Nomad at connect:ID 2017
- NEC software uses facial recognition to verify mobile service users facial-recognition
- Hacker Tracker: New Threats And Old Classics
- IMT And Vislink Display Newsnet Technological Ecosystem at NAB 2017
- For Earth Day, Microsoft outlines its efforts to create smarter, more efficient cities
- Microsoft Ups The Ante In Enterprise IoT and Edge Computing
- Local investment in public safety communications infrastructure pay off during Florida disasters
- Siemens Healthineers makes its mark in population health through Medicalis acquisition
- OneNeck IT Solutions completes HIPAA and HITECH examination
- Federal Engineering to Provide Public Safety Consulting Services To the City of Seattle
- GovTech Founder Series: Founders of Public Safety Software Startup Mark43 on Launching, Long-Term Vision
- Harris Corporation's Global Innovation Center Achieves LEED Silver Certification
- Verizon Invests $1.05 Billion In Fiber Optics
- CompassData's Ground Control and FAA-Certified Airport Data Now Available on Carahsoft

Funding News

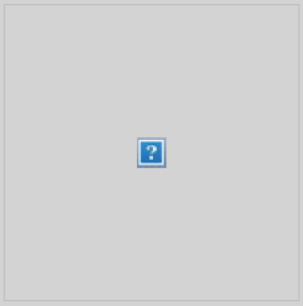
- LoBiondo Announces Nearly $8,000 To Oceanville Fire Company
- Jail Study Points To Alternative Methods For Housing Pretrial Inmates
- Woodstock Police Adopt Body-Worn Cameras
- Portland Secures Funding For Body Camera Pilot Program
- Stark County Sales Tax Renewal: What You Need to Know

- Campbell to Raise Fee for 911 to Pay for New Radio System
- Sheriff Seeks $1.3 Million Technology Upgrade
- McAuliffe Announces $365,000 Federal Grant for Virginia Public Safety Agencies
- Council Approves Financing for Teaneck Road, Votee Park



TIME IS LIMITED ON THESE SOLICITATIONS!

Agency	Project	Status	Release Date	Due Date
Lauderhill Police Department	Wearable Body Cameras	RFP	04/25/2017	05/30/2017
Central Ohio Transit Authority	Electronic Access Control System	RFB	04/25/2017	05/25/2017
Minnesota Department of Human Services	GPS Monitoring System	RFP	04/24/2017	05/19/2017
El Dorado County Information Technologies Department	VMWare Enterprise Software and Production Support	ITB	04/26/2017	05/12/2017
Monroe County Department of Public Safety	Computer Aided Dispatch (CAD) and Mobile Communications	RFP	04/24/2017	06/02/2017



CJIS GROUP is committed to helping you create and execute a winning strategy! ..

- CREATE MESSAGES AND CONTENT THAT RESONATES WITH SLED DECISION MAKERS
- CUSTOMIZE A CAMPAIGN TO MEET YOUR TIMELINE AND OBJECTIVES
- GENERATE PROPRIETARY LEADS BASED ON AUDIENCE RESPONSE TO YOUR MESSAGE

Contact us directly so we can create an solution customized around your 'Go to market' needs. Click the link below to discuss how to **build a better state and local strategy.**

Custom Marketing Services

CJIS GROUP is committed to improving the technology procurement process by providing in depth, validated market intelligence and quality research for the state and local government market.

Sales: 703-822-5089 Support: 850-926-9800

Sales@cjisgroup.com Support@cjisgroup.com



Copyright © 2017 CJIS GROUP LLC
Our address is 1900 Association Drive, Reston, Va 20191, USA

If you do not wish to receive future email, click here.

(You can also send your request to **Customer Care** at the street address above.)

From:	Egnitz, Brian (POL)
To:	peter.p.pouliot.mil@mail.mil
Cc:	Quinn, Dermot (POL); Mason, Christopher (POL); Sojka, Robert (POL)
Subject:	CopLink
Date:	Wednesday, May 10, 2017 11:31:42 AM
Attachments:	BPE MSP CJIS Broker Custom Dev v1.1.pdf BPE MSP Transit COPLINK Integration v3.0.pdf Mass BOP.msg BPE MSP Boston COPLINK Integration v2.0.pdf BPE MSP Citations COPLINK Intg v1.0.pdf

---

Hi Pete,

Per your request, here are some of the CopLink projects that we need funded.

Thanks, Brian

CopLink Enhancements

Project Description:

The Commonwealth of Massachusetts's Fusion Center hosts IBM i2 COPLINK for Local, State and Federal law enforcement agencies. IBM i2 COPLINK is police investigation software that consolidates data from many sources, aids collaboration and helps generate tactical leads quickly. CopLink is used to search record management systems, registry data and criminal history records to solve various crime, such as Homicides, Drug Trafficking and Bank Robberies. This tool provides advanced analytics to law enforcement, data exchange and interoperability to improve connectivity between information sharing systems.

Scope of Work

1. Map the Boston Police Departments Record Management System into CopLink ($28,300)
2. Map the MBTA (Massachusetts Bay Transit Authority) Police Records System into CopLink. ($18,800)
3. Map Lawrence Police Department Record Management System into CopLink (est. $25,000)
4. Map Board of Probation data into CopLink ($22,400)
5. Enhance CopLink to show RMV (Registry of Motor Vehicles) driver's license photos inside of the CopLink software ($63,760)
6. Map the States Automated License Plate Reader Database into CopLink (est. $30,000)
7. Map the States Electronic Citation Database (Civil Motor Vehicle Citation) ($19,850)

Definitions:

A records management system (RMS) is "an agency-wide system that provides for the

storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, or files pertaining to law enforcement operations. RMS covers the entire life span of records development—from the initial generation to its completion. An effective RMS allows single entry of data, while supporting multiple reporting mechanisms." (This definition is taken from both the Bureau of Justice Assistance's Standard Functional Specifications for Law Enforcement Records Management Systems and the International Association of Chiefs of Police [IACP]/Department of Justices' Community Oriented Policing Services [COPS] Technology Technical Assistance Program's Records Management Systems documents.)

"Records" are the information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business. The International Council on Archives (ICA) Committee on Electronic Records defines a record as, "recorded information produced or received in the initiation, conduct or completion of an institutional or individual activity and that comprises content, context and structure sufficient to provide evidence of the activity."

BOP database contains Criminal Offender Record Information, which consists of records and data in any communicable form compiled by a Massachusetts criminal justice agency about an identifiable individual that relate to:

- Nature or disposition of a criminal charge,
- An arrest,
- A pre-trial proceeding,
- Other judicial proceedings,
- Sentencing,
- Incarceration,
- Rehabilitation,
- Release

Automated License Plate Recognition (ALPR) is a technology that uses optical character recognition (OCR) to automatically read license plate characters.

There are two types of ALPR: stationary, which uses infrared (IR) cameras at high fixed points, and mobile, which uses vehicle-mounted IR cameras.

Stationary cameras can be mounted on signs, street lights, highway overpasses or buildings as a cost-effective way to monitor moving and parked vehicles twenty-four hours a day. Camera software is able to identify the pixel patterns that make up a license plate and translate the letters and numbers on the plate to a digital format. The plate data is then sent to a database where it is compared in real-time to a list of plate numbers that belong to "vehicles of interest". If the system detects a match, it sends an alert to the dispatcher or other designated personnel.

Mobile ALPR software suites use multiple cameras mounted on a vehicle. As the vehicle moves, it photographs license plates and transmits plate data to a database. The database may be a national database or it may be created at the local level and downloaded into the vehicle's onboard computer at the beginning of each shift. If the system detects a match,

the officer receives an alert on his computer. A mobile ALPR can read up to 1,000 plates per hour and cover two or more lanes of traffic at once.

Automated License Plate Recognition has many uses including:
•Recovering stolen cars.
•Identifying drivers with an open warrant for arrest.
•Catching speeders by comparing the average time it takes to get from stationary camera A to stationary camera B.
•Determining what cars do and do not belong in a parking garage.
•Expediting parking by eliminating the need for human confirmation of parking passes.

ALPR is known by several other names, including Automatic Number Plate Recognition (ANPR), Automatic Vehicle Identification (AVI), Car Plate Recognition (CPR), License Plate Recognition (LPR), and Lecture Automatique de Plaques d'Immatriculation (LAPI).

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7216 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

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

From: Terri Clark
To: Terri Clark
Subject: CT Academy - CVISN EScreening - Additional Presentation Materials
Date: Wednesday, February 22, 2017 8:09:53 AM
Attachments: DIRECTIONS to CASE.pdf
AGENDA CASE CVISN EScreening Study Committee Meeting 2 22 17.pdf
CASE SRI 02 22 17 presentation.pdf
CASE - CT CVISN Trucks BMason pptx.pdf

REMINDER: STUDY COMMITTEE MEETING

- See additional electronic presentation materials attached.

TO: CT Academy – CVISN Escreening Study Committee

The next meeting of the CT Academy – CVISN Escreening Study Committee is as follows:

WHEN: Wednesday, February 22, 2017

TIME: 9:00 am – 12:00 pm EST

LOCATION: CASE Offices, 805 Brook Street, Building 4 – CERC, Rocky Hill (see directions attached)

AGENDA: See Attached

TELECONFERENCE IS AVAILABLE:
Dial: 866-740-1260
Access: 5272161#

Please see attached:

- Agenda Item: Sam Fayez, Director, Transportation and Logistics
- Agenda Item: Barry Mason, Study Manager

Best regards -

Terri Clark
Associate Director
Connecticut Academy of Science and Engineering
805 Brook Street, Building 4-CERC
Rocky Hill, CT 06067-3405
860/571-7143
mailto:tclark@ctcase.org

From: Terri Clark
To: Terri Clark
Subject: CT Academy - CVISN EScreening - Electronic Meeting Materials Attached
Date: Tuesday, May 23, 2017 1:10:10 PM
Attachments: DIRECTIONS to CASE.pdf
CASE - CVISN E-Screening IIS Presentation 05 24 17.pdf
CASE – CVISN E-SCREENING STUDY UPDATE 05 24 17.pdf
CASE - CVISN E-Screening UNR Presentation 05 24 17.pdf
AGENDA CASE CVISN EScreening Study Committee Meeting 05 24 17.pdf

---

REMINDER: STUDY COMMITTEE MEETING

- See attached presentation materials
  Guest Presentations: IIS and University of Nevada
  CASE Study Update
- Monitor you email up through the time of the meeting for additional electronic presentation materials

TO: CT Academy – CVISN Escreening Study Committee

The next meeting of the CT Academy – CVISN Escreening Study Committee is as follows:

WHEN: Wednesday, May 24, 2017

TIME: 9:00 am – 12:00 pm EST

LOCATION: CASE Offices, 805 Brook Street, Building 4 – CERC, Rocky Hill (see directions attached)

AGENDA: *See Attached*

TELECONFERENCE IS AVAILABLE:
Dial: 866-740-1260
Access: 5272161#

Best regards -

Terri Clark
Associate Director
Connecticut Academy of Science and Engineering
805 Brook Street, Building 4-CERC
Rocky Hill, CT 06067-3405
860/571-7143
mailto:tclark@ctcase.org

From: Traffic Technology Today
To: Dowd, Timothy (POL)
Subject: DSRC-based connected V2X technology to be showcased at 2017 ITS World Congress
Date: Friday, October 20, 2017 6:00:35 AM

If you are having trouble viewing this email, click here to display it in your web browser

NEW AUDIO: Managing the risks of introducing new traffic technologies

Veronique (Ronnie) Hakim, managing director of New York's Metropolitan Transportation Authority (MTA), was recently inducted into ITS New Jersey's Hall of Fame for her many years of managing and enhancing the state's transportation systems. In this clip with Transportation Radio's Bernie Wagenblast, Hakim explains why her approach to adopting untried traffic technologies is 'leading edge, not bleeding edge' more...

NEW VIDEO: How new autonomous vehicles interact with traffic and pedestrians

As autonomous vehicle technology improves, so the picture they build up of the world around them is becoming more detailed. This new video from Nvidia gives us insight into the image processing and machine learning that occurs within its latest autonomous vehicle hardware, thereby helping traffic managers to understand the how such technology works, and how it may be useful for improving safety and for 3D map making more...

For more of the latest multimedia reports visit our Video & Audio homepage here.

Top news stories this week

DSRC-based connected V2X technology to be showcased at 2017 ITS World Congress

Co-hosts ITS America and ITS Canada have announced that the 2017 ITS World Congress will showcase connected and autonomous vehicles (CAVs) integrated with dedicated short-range communications systems (DSRC) in order to demonstrate the benefits of the technology **more...**

More news...

Governors sign MOU to plan regional EV corridor across seven western US states

Kapsch presents smarter transport and tolling systems at IBTTA International Summit

Oregon awarded USDOT grants to expand RUC program and trial bi-state system

Merge consortium says a third of London car journeys could be replaced by AVs by 2025

Balfour Beatty Mott MacDonald extends Highways England maintenance contract

Danlaw to supply DSRC Aftermarket Safety Devices for UMTRI connected vehicle program

All Traffic Solutions launches new all-in- one ALPR camera system

Australian study shows connected and automated driving could reduce road injuries

Swarco Traffic to demonstrate two new products at Road Expo Scotland

TomTom to develop new Hub and Michelin's app for truckers

Indra starts Madrid CAV trials as part of the European AutoCITS project

Buchanan Computing publishes latest UK government crash data on its CollisionMap

NEW monthly poll

Last month UK transportation industry watchdog Transport Focus told Highways England it should do more to educate the public about smart motorways – the congestion-slashing freeway system of dynamic speed limits and all-lane running (read more here)

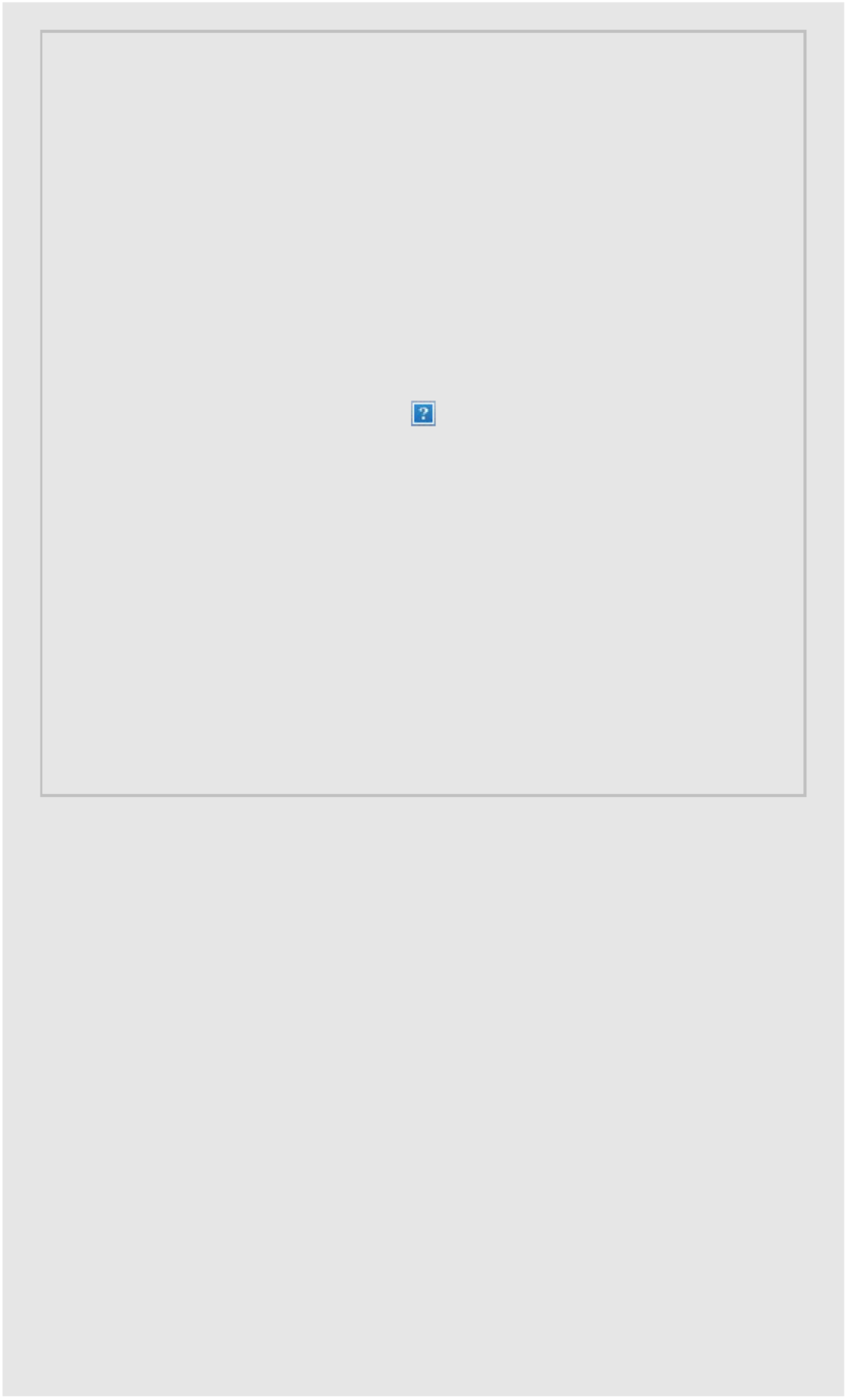
Do you think dynamic speed limits and all-lane running are poorly understood by the public and road authorities should invest in promoting them more?

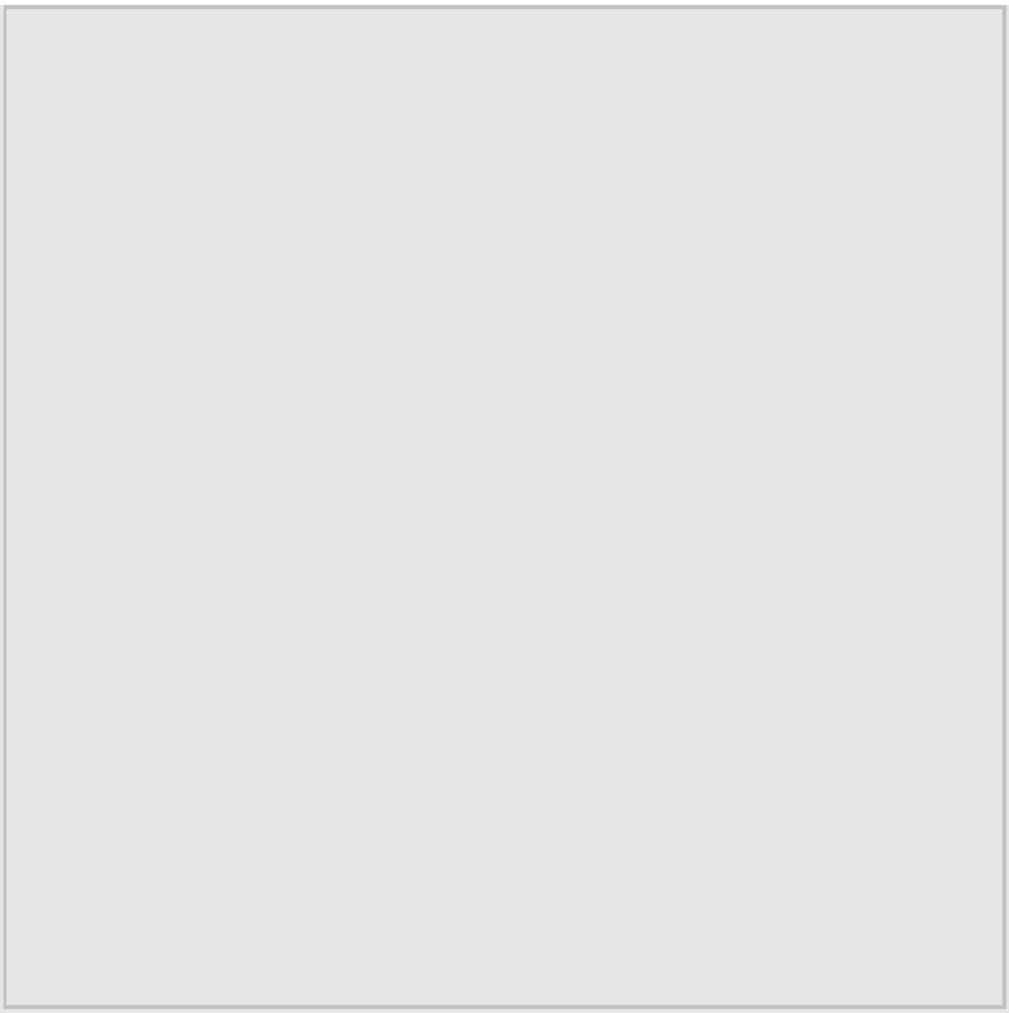
• Yes, safety and compliance will be improved with better education

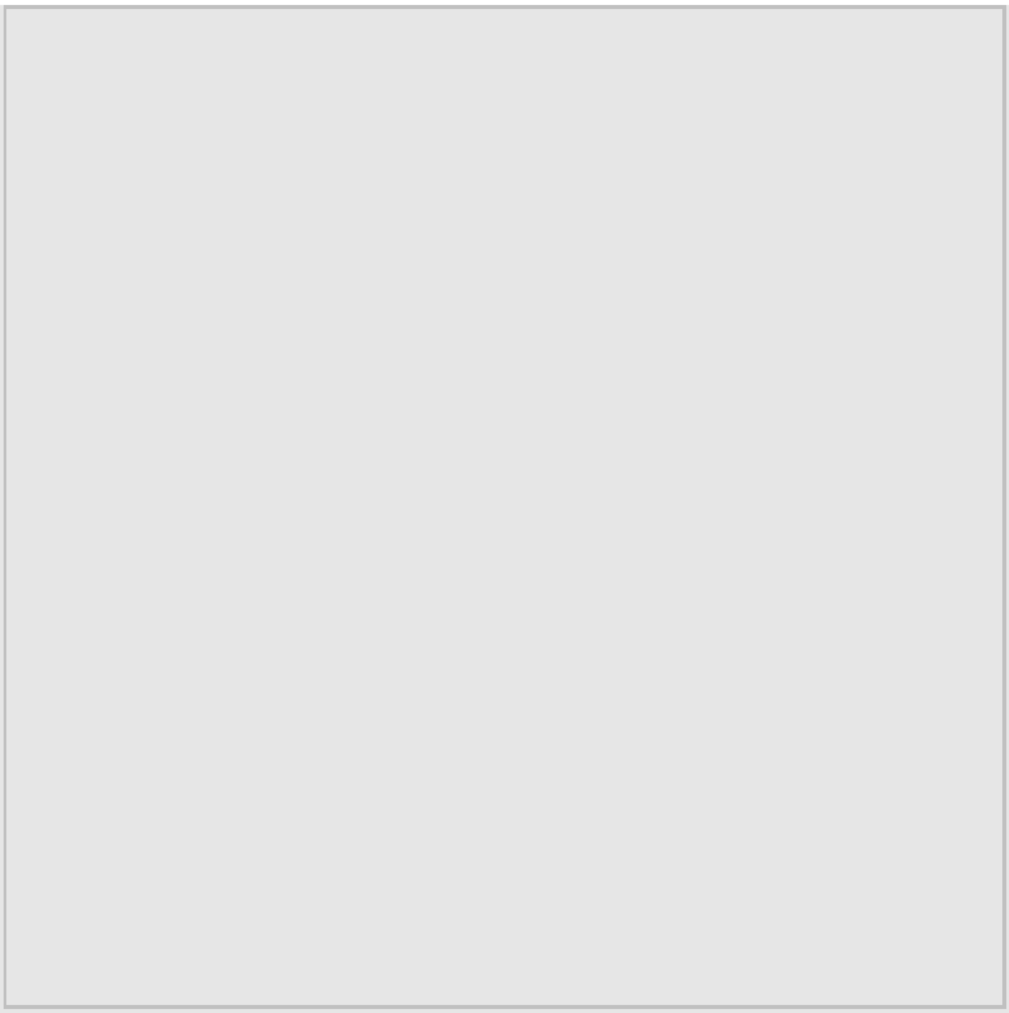
• No, dynamic speed limits already work well – money would be better spent on further road improvements

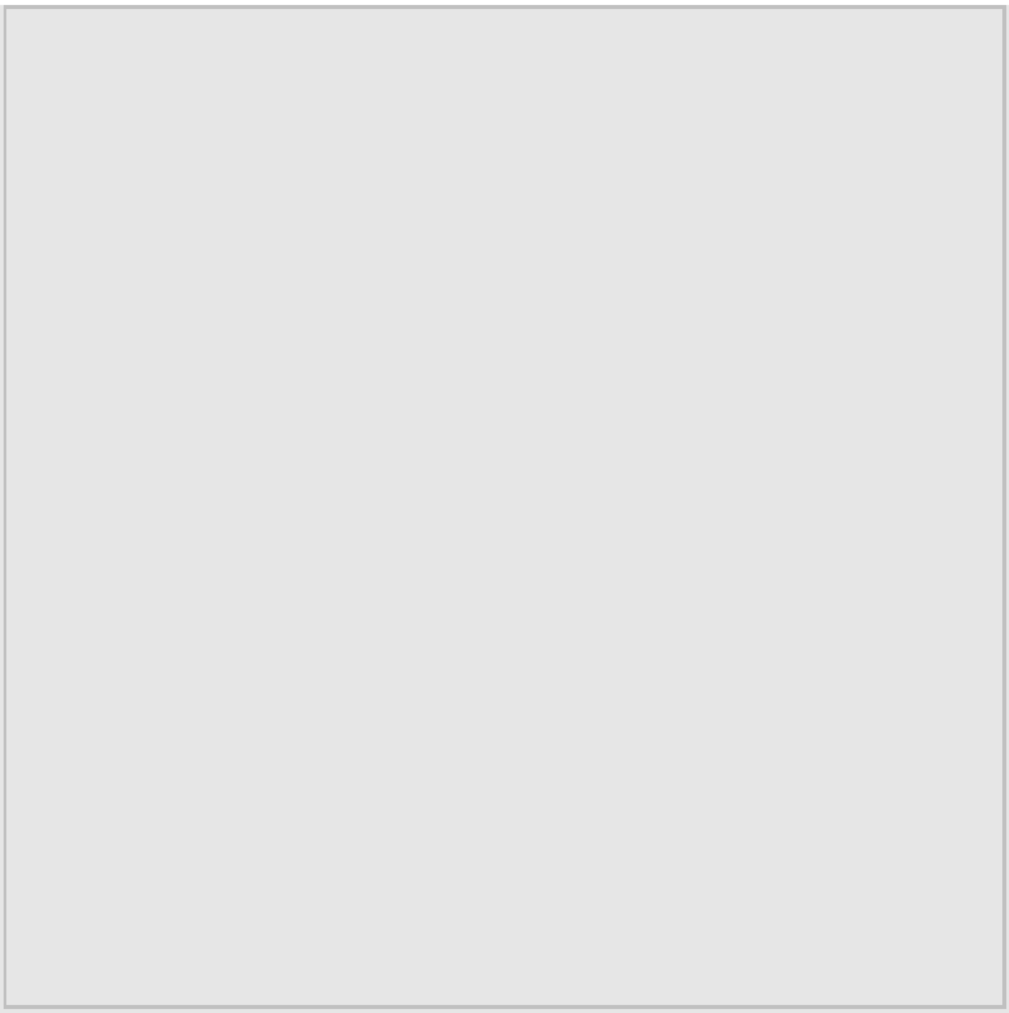
Click here to vote now!

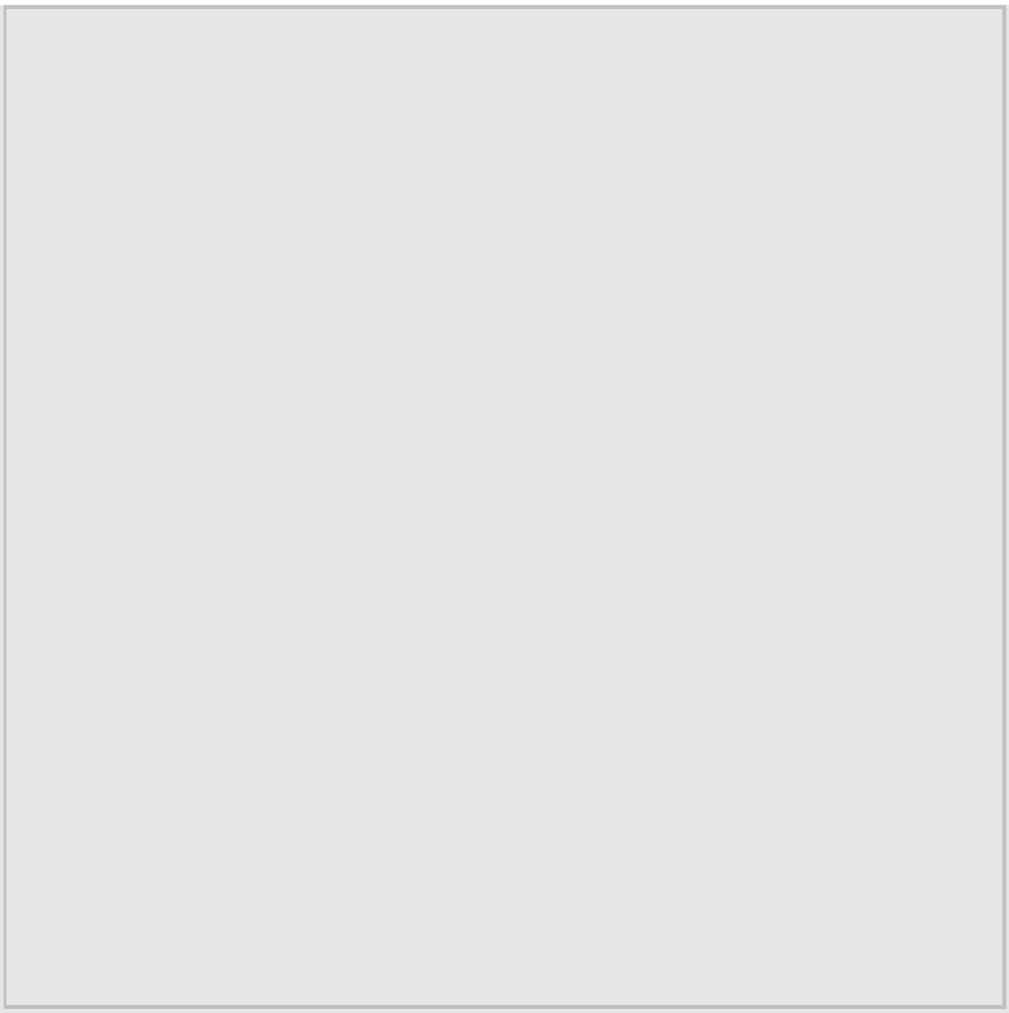
The results so far show...

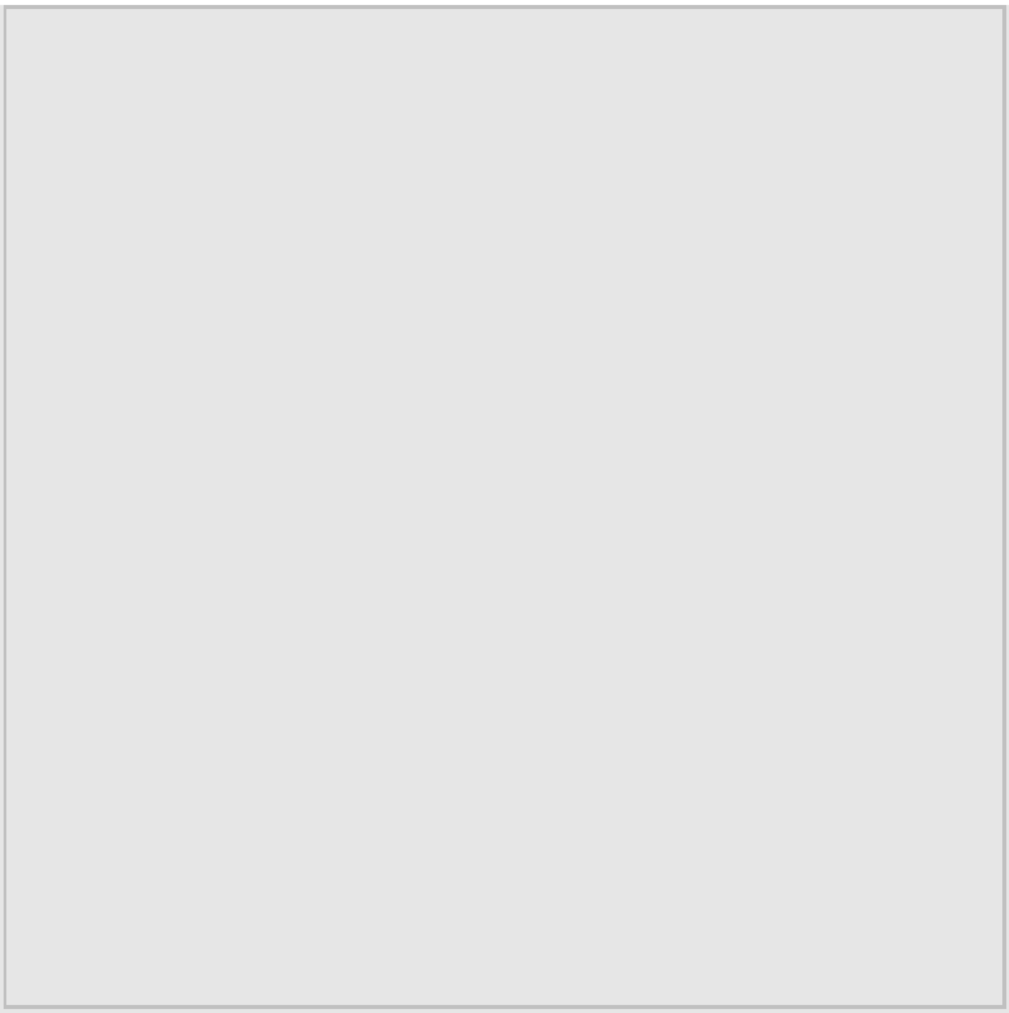


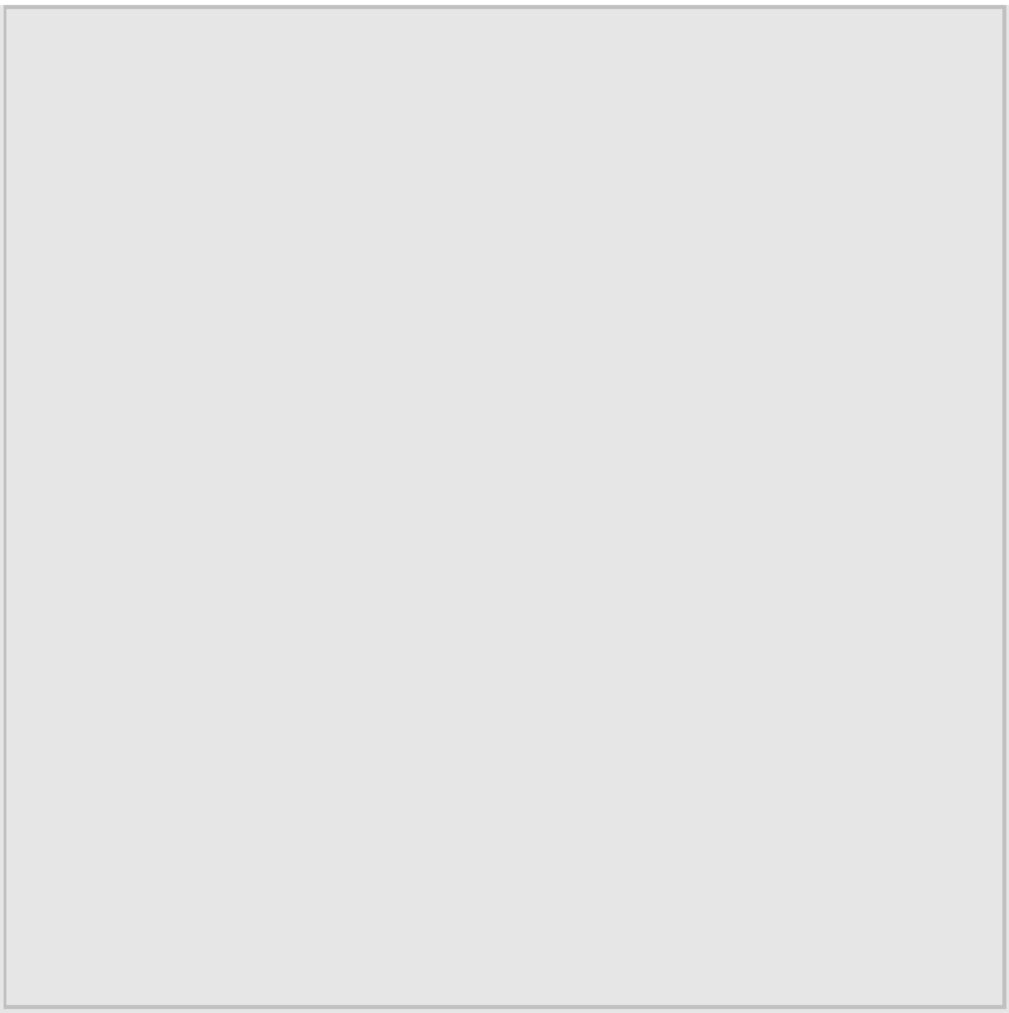












Inside this issue...



<< COVER STORY

5G: THE GAME CHANGER

Everyone interested in connected vehicles wants to know exactly what the promised, blazingly fast 5G network will be capable of. Now researchers in Finland are beginning to find out as they build a prototype deployment, and investigate potential real-world road traffic use cases.

<< ENHANCED ENFORCEMENT

FUTURE FACING

With the launch of Apple's new iPhone X, facial recognition technology has been propelled into the mainstream. How long then, asks James Gordon, will it be before road authorities begin relying on it for traffic enforcement?



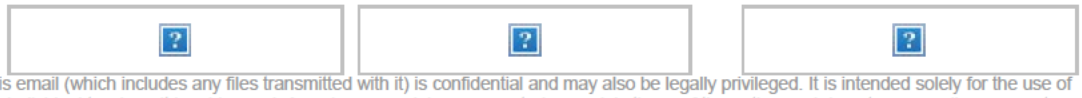
<< V2X DEPLOYMENT

NEW CONNECTIONS

David W Smith speaks to state DOTs in the USA about the challenges of deploying connected-vehicle infrastructure, and finds out about the solutions that are being worked on now, and planned for the future.

Click to view your copy online NOW!





This email (which includes any files transmitted with it) is confidential and may also be legally privileged. It is intended solely for the use of the individual to whom it is addressed. Any views or opinions presented are solely those of the author and do not necessarily represent those of UKi Media & Events. If you are not the intended recipient, be advised that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited. If you have received this message in error, do not open any attachment but please notify the sender (above) deleting this message from your system. Please rely on your own anti-virus system, no responsibility is taken by the sender for any damage rising out of virus infection.

UKi Media & Events, a division of UKIP Media & Events Limited
Registered Address: 26 Red Lion Square, London, WC1R 4AG
VAT No. GB879 4451 71
Registration Number: 5893940
Company registered in England and Wales

From: Traffic Technology Today
To: Dowd, Timothy (POL)
Subject: DSRC-based connected V2X technology to be showcased at 2017 ITS World Congress
Date: Friday, October 20, 2017 6:00:38 AM

If you are having trouble viewing this email, click here to display it in your web browser

NEW AUDIO: Managing the risks of introducing new traffic technologies

Veronique (Ronnie) Hakim, managing director of New York's Metropolitan Transportation Authority (MTA), was recently inducted into ITS New Jersey's Hall of Fame for her many years of managing and enhancing the state's transportation systems. In this clip with Transportation Radio's Bernie Wagenblast, Hakim explains why her approach to adopting untried traffic technologies is 'leading edge, not bleeding edge' more...

NEW VIDEO: How new autonomous vehicles interact with traffic and pedestrians

As autonomous vehicle technology improves, so the picture they build up of the world around them is becoming more detailed. This new video from Nvidia gives us insight into the image processing and machine learning that occurs within its latest autonomous vehicle hardware, thereby helping traffic managers to understand the how such technology works, and how it may be useful for improving safety and for 3D map making more...

For more of the latest multimedia reports visit our Video & Audio homepage here.

Top news stories this week

DSRC-based connected V2X technology to be showcased at 2017 ITS World Congress

Co-hosts ITS America and ITS Canada have announced that the 2017 ITS World Congress will showcase connected and autonomous vehicles (CAVs) integrated with dedicated short-range communications systems (DSRC) in order to demonstrate the benefits of the technology **more...**

More news...

Governors sign MOU to plan regional EV corridor across seven western US states

Kapsch presents smarter transport and tolling systems at IBTTA International Summit

Oregon awarded USDOT grants to expand RUC program and trial bi-state system

Merge consortium says a third of London car journeys could be replaced by AVs by 2025

Balfour Beatty Mott MacDonald extends Highways England maintenance contract

Danlaw to supply DSRC Aftermarket Safety Devices for UMTRI connected vehicle program

All Traffic Solutions launches new all-in- one ALPR camera system

Australian study shows connected and automated driving could reduce road injuries

Swarco Traffic to demonstrate two new products at Road Expo Scotland

TomTom to develop new Hub and Michelin's app for truckers

Indra starts Madrid CAV trials as part of the European AutoCITS project

Buchanan Computing publishes latest UK government crash data on its CollisionMap

NEW monthly poll

Last month UK transportation industry watchdog Transport Focus told Highways England it should do more to educate the public about smart motorways – the congestion-slashing freeway system of dynamic speed limits and all-lane running (read more here)

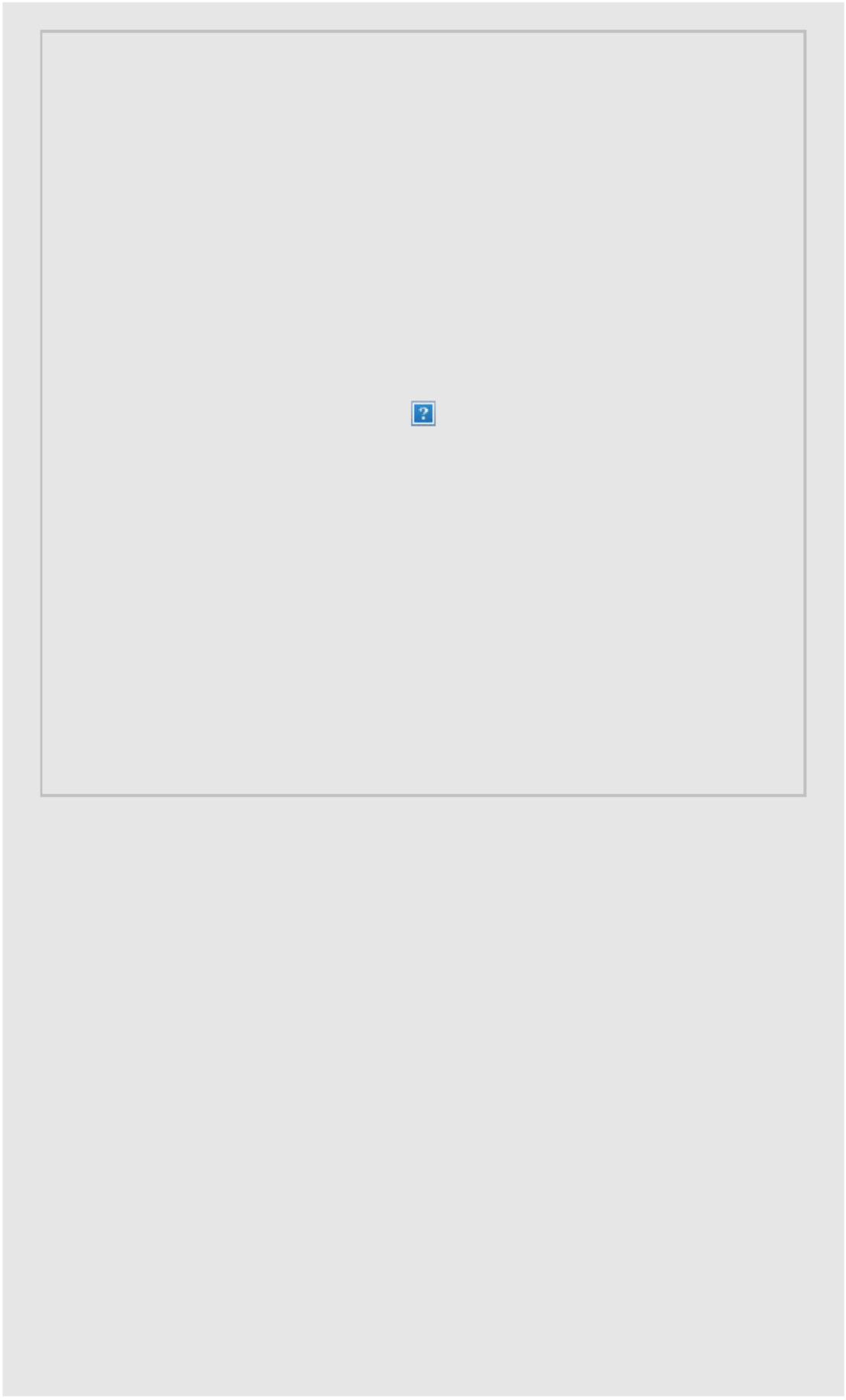
Do you think dynamic speed limits and all-lane running are poorly understood by the public and road authorities should invest in promoting them more?

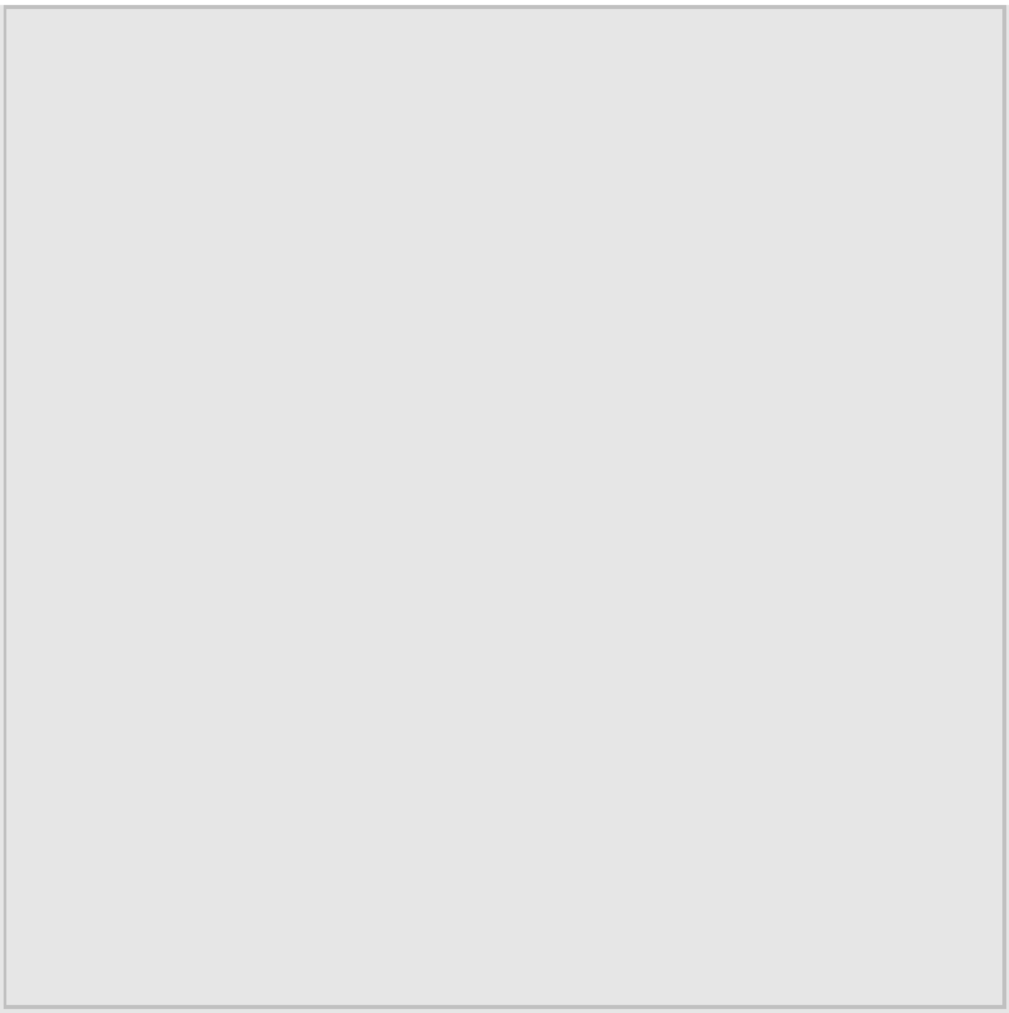
• Yes, safety and compliance will be improved with better education

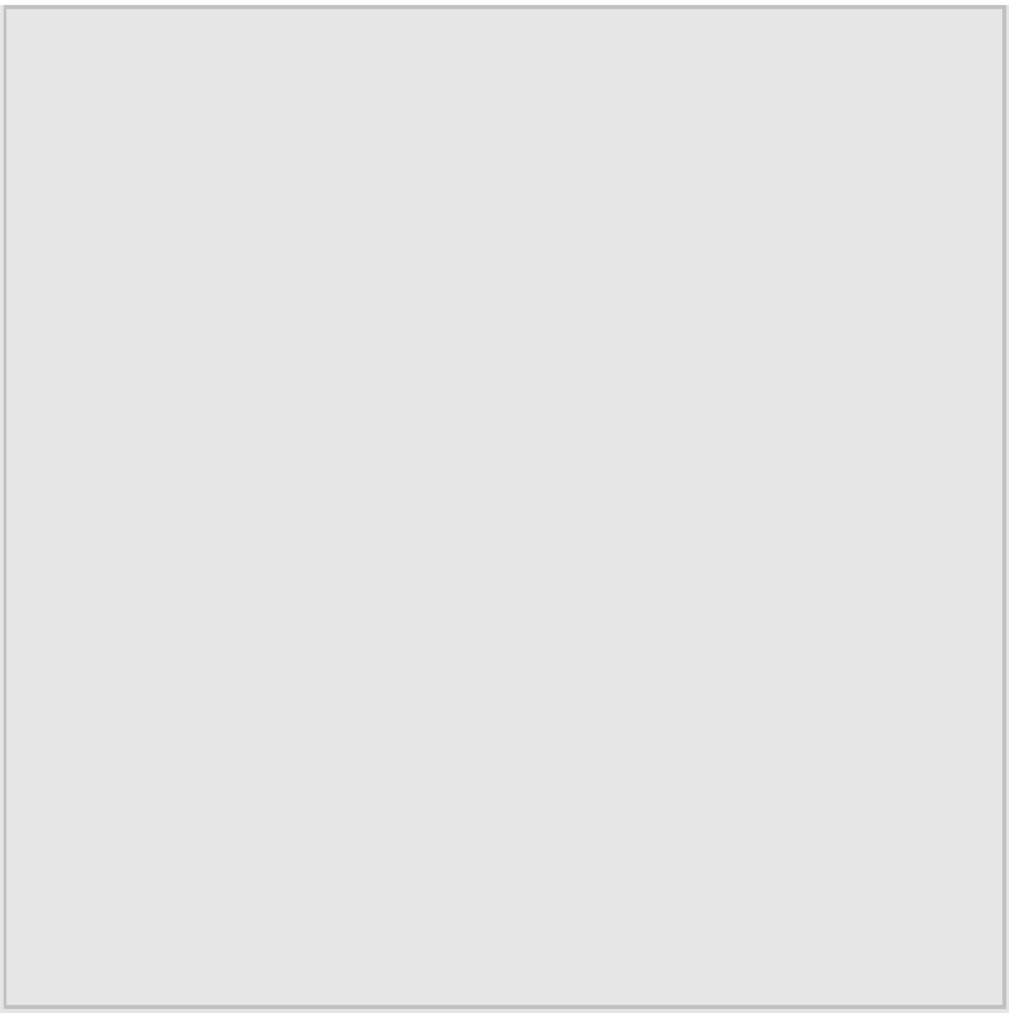
• No, dynamic speed limits already work well – money would be better spent on further road improvements

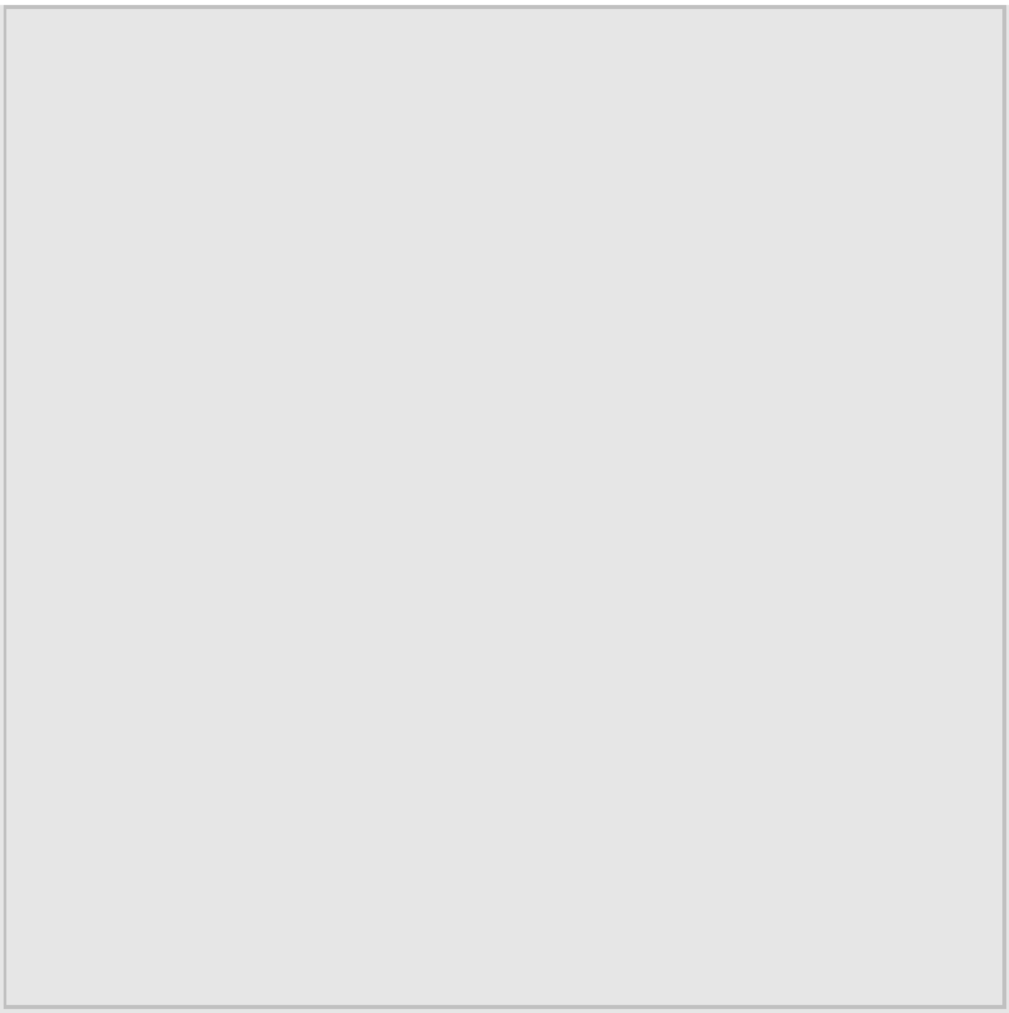
Click here to vote now!

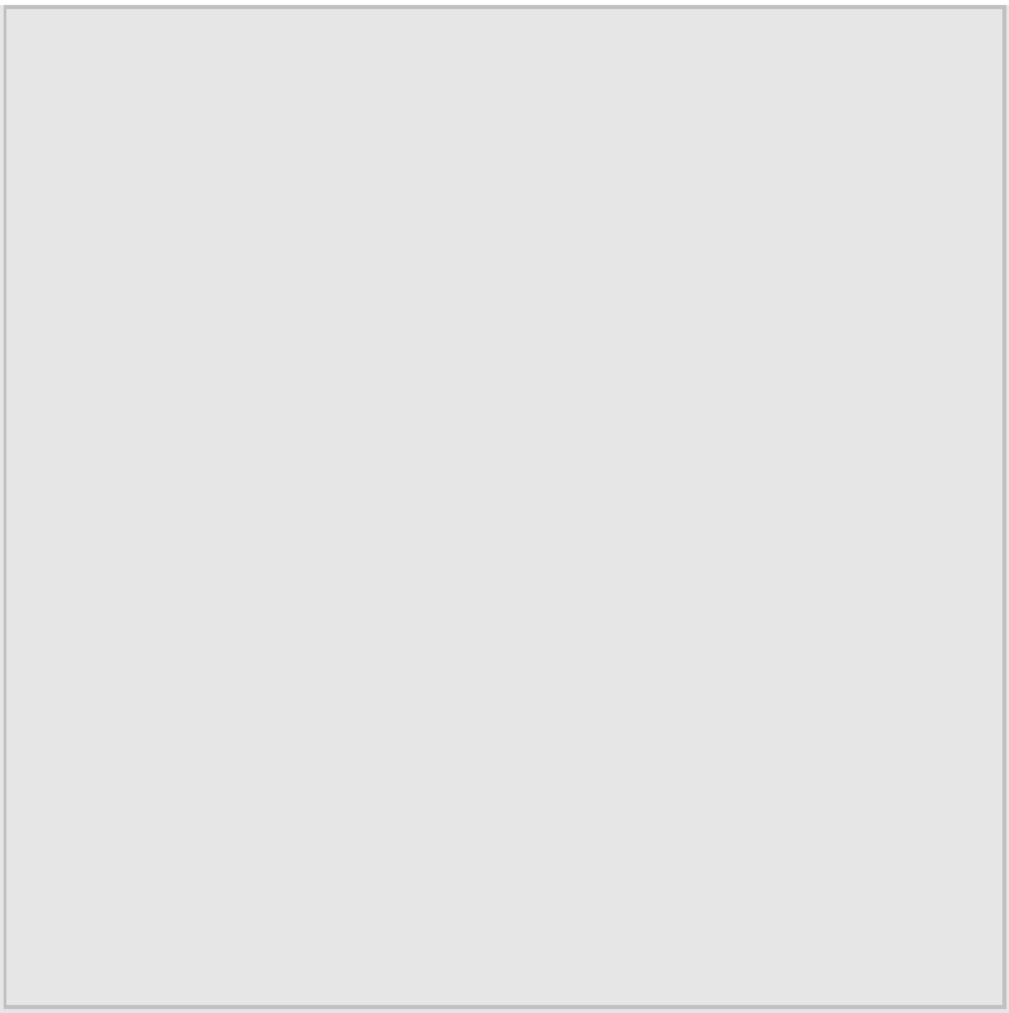
The results so far show...

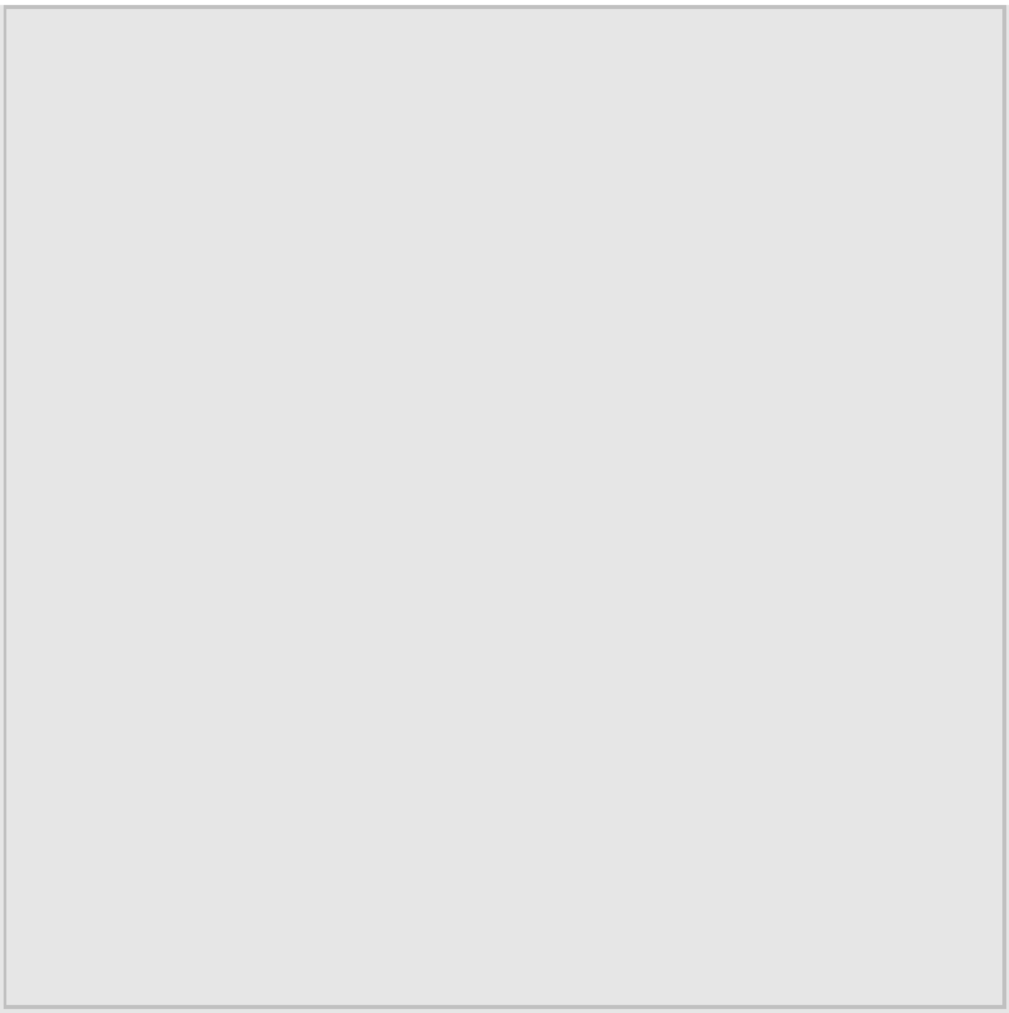


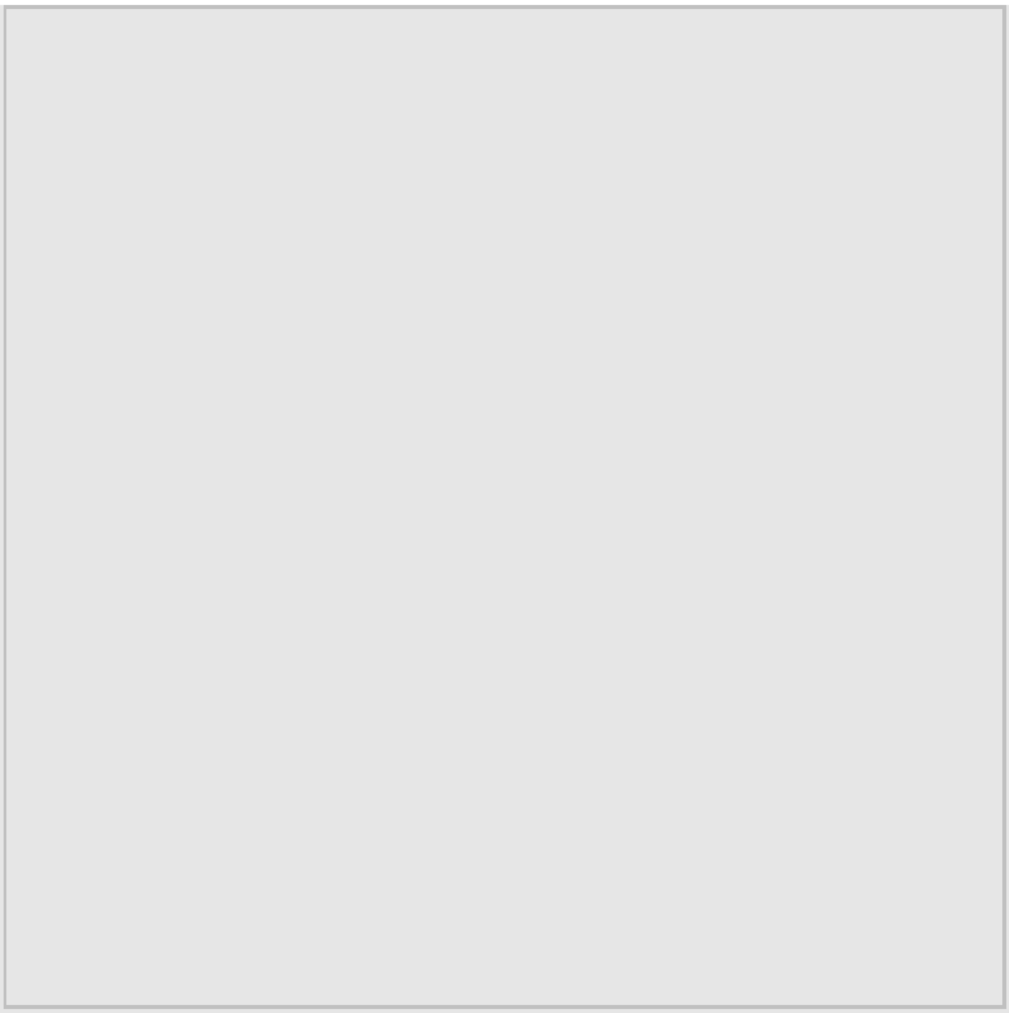












Inside this issue...



<< COVER STORY

5G: THE GAME CHANGER

Everyone interested in connected vehicles wants to know exactly what the promised, blazingly fast 5G network will be capable of. Now researchers in Finland are beginning to find out as they build a prototype deployment, and investigate potential real-world road traffic use cases.

<< ENHANCED ENFORCEMENT

FUTURE FACING

With the launch of Apple's new iPhone X, facial recognition technology has been propelled into the mainstream. How long then, asks James Gordon, will it be before road authorities begin relying on it for traffic enforcement?



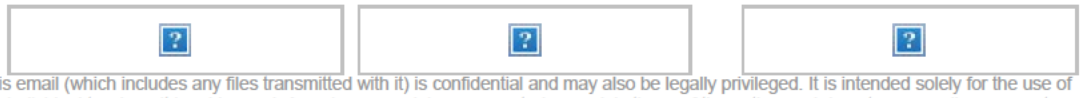
<< V2X DEPLOYMENT

NEW CONNECTIONS

David W Smith speaks to state DOTs in the USA about the challenges of deploying connected-vehicle infrastructure, and finds out about the solutions that are being worked on now, and planned for the future.

Click to view your copy online NOW!





This email (which includes any files transmitted with it) is confidential and may also be legally privileged. It is intended solely for the use of the individual to whom it is addressed. Any views or opinions presented are solely those of the author and do not necessarily represent those of UKi Media & Events. If you are not the intended recipient, be advised that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited. If you have received this message in error, do not open any attachment but please notify the sender (above) deleting this message from your system. Please rely on your own anti-virus system, no responsibility is taken by the sender for any damage rising out of virus infection.

UKi Media & Events, a division of UKIP Media & Events Limited
Registered Address: 26 Red Lion Square, London, WC1R 4AG
VAT No. GB879 4451 71
Registration Number: 5893940
Company registered in England and Wales

From: Nathan Maloney
To: Guen, John (POL)
Subject: ELSAG eNews - June 2017
Date: Tuesday, June 27, 2017 12:01:24 PM

Welcome to ELSAG's e-newsletter, The ALPR Record, keeping you informed about ELSAG news, events, products and other information you need as ELSAG customers. Thank you for reading.

June 2017

Long Beach PD Keeps An Eye On Who Comes To Town

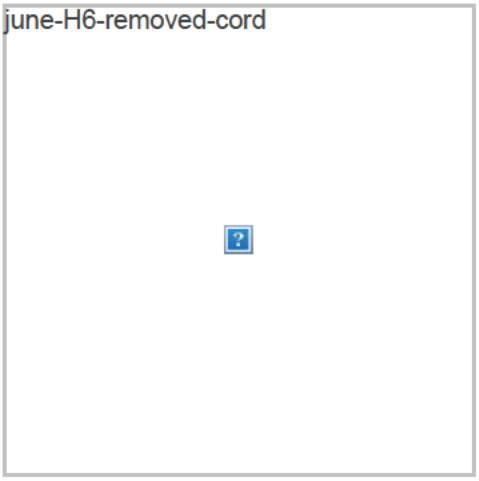
June-fixed-camera2.jpg

Long Beach, NY plans to install our Plate Hunter™ ALPR systems at the site of every traffic lane entering the city. Having used our ALPR technologies since 2006, and realizing a significant improvement in public safety as a result, the Long Beach Police Department self-funded the new systems as part of the city's 2016 capital improvement plan. For details given by Police Commissioner Michael Tangney and City Councilman Scott Mandel, click the

button below.

Get Low Cost, High Performance with the Plate Hunter™ H6 ALPR System

Our Plate Hunter H6™ ALPR system is a lower cost, fixed solution which uses the smaller, less overt cameras of our mobile Plate Hunter M6™ system, without sacrificing amazing speed and accuracy that define our ALPR technologies. The H6™ is ideal for monitoring access control, parking enforcement and keeping a watch over urban environments with 1-2 lanes of coverage, and in other areas where vehicles have limited or restricted movement.



PERFORMANCE OF THE PLATE HUNTER H6™ :

- Cameras read license plates, day or night, in any weather
- Recognizes plates using specially designed protocols for each jurisdiction in which the systems are deployed
- Captures date and time stamps, GPS coordinates and photo of the license plate
- Each license plate read can be compared to a hot list to identify suspect vehicles
- Hot lists can be updated remotely as often as needed
- Broadcasts suspect vehicle alarms to command centers or patrol cars simultaneously; broadcasts to an in-car computer, email or PDA
- Issues multi-level alarms for prioritization—Wants, Warrants, AMBER Alerts, etc.
- All data collected by the H6™ can be archived in ELSAG's EOC database and analyzed to aid investigations

Maximize your efficiency by delegating some tasks the Plate Hunter™ H6 ALPR system. Contact us to discuss how this versatile, low cost solution can assist your law enforcement missions.

info@elsag.com / elsag.com

Team Member Spotlight: Rose Williams

It takes a lot of focus and organization behind the scenes to keep our company running efficiently. Rose Williams has served us as an Accounts Payable and Receivable Accountant for nearly a decade, tending to the tedious details involved with ensuring our books are in order. Rose has established excellent working relationships with our customers and vendors, always happy to answer account questions and investigate answers, if needed. Her diligence has not just exceeded our expectations and performance goals, but Rose's contributions to our company have had a positive influence on our bottom line. Rose is the ultimate team player and when asked about why she enjoys working her, she shared,

"I feel valued here and I also believe that our defense technologies are improving the quality of work by our leaders and law enforcement officials by allowing them to better protect and secure our country and others around the world."



Look for ELSAG at these upcoming conferences:

June 27 - 28
NJ Police Expo
Atlantic City, NJ

July 23 - 24
PA Police Chief's Conference
Camp Hill, PA

July 18 - 20
NATIA
Tampa, FL

August 2 - 6
NAWLEE
Kansas City, MO

July 23 - 27
KY Police Chiefs
Paducah, KY

August 13 - 17
MVCI Conference
Atlanta,GA



Current versions of ELSAG ALPR Technologies

CarSystem™ 6.12 and Enterprise Operations Center™ 5.6

For optimal performance of your ELSAG ALPR systems, it is imperative that your hardware and software are up-to-date. Compatibility between the CarSystem™ and Enterprise Operations Center™ server are critical, whether or not you manage your own ALPR server. If your ELSAG ALPR systems are within warranty and you have not yet installed the current CarSystem™ and EOC™ versions, or if you need to update your warranty to take advantage of the most current ALPR technologies, please call our Help Desk at 866-967-4900.

For more information please email info@elsag.com. For Warranty Support please email warrantywizard@elsag.com.

This publication is issued to provide outline information only and is supplied without liability for errors or omissions. No part of it may be reproduced or used unless authorized in writing. We reserve the right to modify or revise all or part of this document without notice.

2017 © Copyright ELSAG

ELSAG License Plate Recognition Systems are manufactured by Selex ES Inc., a Leonardo company.

4221 Tudor Lane Greensboro NC 27410-8105 | Tel: 1(877) 773.5724 | www.elsag.com

You received this email because you are subscribed to Marketing Information from ELSAG.

Update your email preferences to choose the types of emails you receive.

Unsubscribe from all future emails

From: P1 Leadership Product Alerts
To: McCarthy, Steven (POL)
Subject: ELSAG is now LEONARDO!
Date: Thursday, September 14, 2017 12:42:55 PM

Having trouble viewing this email? View it in your browser.

Over the coming months, when you see the LEONARDO brand mark, know that's us! Our parent company has been renamed LEONARDO and we're taking on that name too, in all our branding! But the name ELSAG is dear to us and recognized by our customers worldwide, so we've given it a new job by incorporating it into our product names. Our Mobile Plate Hunter™ ALPR system is now the ELSAG Mobile Plate Hunter and our Fixed Plate Hunter™ ALPR system is now the ELSAG Fixed Plate Hunter, and so on.

So that's the news from here! Your LEONARDO team is comprised of the same great people, running the same great company, making the same great ELSAG Plate Hunter™ ALPR technologies, serving the greatest customers on Earth. We're still transitioning into our new brand so please help us pass on the news at the water cooler or over lunch with your associates that ELSAG is now LEONARDO.

For information about LEONARDO's versatile, force-multiplying ELSAG Plate Hunter ALPR technologies that aid every mission involving a vehicle, from identifying unlicensed drivers to recovering stolen vehicles to finding missing persons to locating a get-away vehicle to supporting Homeland Security missions, and so much more, please reach out to us at 1 (877) 773.5724 or visit leonardocompany-us.com and click on Law Enforcement Systems.



If you do not wish to receive future PoliceOne Product Alerts, please unsubscribe.
To change your email address, update your profile. © 2017: PoliceOne.com. All Rights Reserved.
200 Green Street, 2nd Floor, San Francisco, CA 94111



From: Mason, Christopher (POL)
To: Mason, Christopher (POL)
Subject: Emailing: ALPR Law Enforcement Dept Model Policy - Final 20131008
Date: Tuesday, February 14, 2017 2:56:11 PM
Attachments: ALPR Law Enforcement Dept Model Policy - Final 20131008.pdf

---

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

ALPR Law Enforcement Dept Model Policy - Final 20131008

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

From: Egnitz, Brian (POL)
To: Mason, Christopher (POL)
Cc: Crouse, David (POL)
Subject: EOTSS - Meeting Notes
Date: Thursday, November 16, 2017 11:06:00 AM

On 10/30/2017, I hosted a meeting with Sean Hughes, Matt Stockwell and Tim Mitchell from EOTSS. I requested the meeting to discuss ongoing technology support concerns and upcoming projects. Present at the meeting and assisting was Sgt. Dave Crouse.

The following Items were discussed:

a. The 3M Boss ALPR system is not purging after 1 year and data exists in the system beyond the 1 year retention policy. An action item was identified and Tim was to contact the vendor to get support. I proactively contacted the vendor that day, Mike Roth via email and requested that he review the purge problem and work to resolve it. Sean was previously notified via email on 9/7/2017 about this issue and I used this meeting to follow up on the resolution. As of the 11/16/2017 purging of data is not occurring.
b. The existing dedicated hardware hosted at the Chelsea Data Center used to host MSP virtual servers and related applications is getting near end of life and new hardware needs to be procured or existing services and servers need to be migrated into comingled hardware environments. An action item was identified:
    i. Identify server specs for ACISS SQL. ACISS was contacted on 10/31/2017 for specs, a reminder was sent on 11/16/17. As of 11/16/17 no server specs have been provided.
c. The MSP 2010 SharePoint is becoming end of life and needs to be decommissioned or upgraded. An action item was identified:
    i. Tim will get a contact for Stonewall, the EOPSS SharePoint contractor and we will set up a meeting to discuss migrating the MSP 2010 SharePoint Environment into the EOPSS 2013 SharePoint Environment. A follow up email was sent to Tim on 10/31/2017. As of 11/16/17, no contact with Stonewall has been made.
d. A request for Cloud guidance was made; new cloud offerings are being made to us by existing and new vendors regularly. I requested information on what standard the solutions should be held to, Gov cloud, CJIS requirements etc. No action item was identified. No guidance was made available.
e. The CCU backup project was discussed and I recommended moving the CCU backup files to the Amazon Gov cloud for Disaster Recovery. An action item was identified to forward the final quote to Sean for further review. Sean also recommended we do a Vendor background check. On 10/30/2017 I reached out to Todd, our POC at Smartronix and asked if we could do a vendor background check, Todd said the team doing the services would submit to a CORI check. A request was made to Sean on 10/31/2017 for the vendor forms and guidance. As of 11/16/17, no response has been received.
f. Lastly, I advised the EOTSS team on the single point of failure within the TSU and requested additional assistance to support. Both covert and overt

video management solutions and the Systech wiretap system rely on one Trooper to maintain the applications, upgrades, routing and, networking, active directory, group policy, servers, storage and workstations. No action items were identified

-Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7216 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

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

From: Terri Clark
To: Terri Clark; Terri Clark; Terri Clark; Terri Clark
Subject: FW: CT Academy - CVISN EScreening - Electronic Meeting Materials Attached
Date: Wednesday, May 24, 2017 8:45:25 AM
Attachments: DIRECTIONS to CASE.pdf
CASE - CVISN E-Screening IIS Presentation 05 24 17.pdf
CASE – CVISN E-SCREENING STUDY UPDATE 05 24 17.pdf
CASE - CVISN E-Screening UNR Presentation 05 24 17.pdf
AGENDA CASE CVISN EScreening Study Committee Meeting 05 24 17.pdf
CASE CTDOT WIM Status Traffic Monitoring.pdf

NOTE: See additional electronic presentation materials – CASE CTDOT WIM Status – for today's meeting.

Additionally, all electronic presentation materials for today's meeting that were previously send have been re-attached for your convenience.

Best regards –

Terri Clark, Associate Director
Connecticut Academy of Science and Engineering
805 Brook Street, Building 4-CERC
Rocky Hill, CT 06067-3405
860/571-7143, tclark@ctcase.org

From: Terri Clark
Sent: Tuesday, May 23, 2017 1:05 PM
To: CASE - CVISN ESCREENING - Study Committee <tclark@ctcase.org>
Subject: CT Academy - CVISN EScreening - Electronic Meeting Materials Attached

REMINDER: STUDY COMMITTEE MEETING

- See attached presentation materials
  Guest Presentations: IIS and University of Nevada
  CASE Study Update
- Monitor you email up through the time of the meeting for additional electronic presentation materials

TO: CT Academy – CVISN Escreening Study Committee

The next meeting of the CT Academy – CVISN Escreening Study Committee is as follows:

WHEN: Wednesday, May 24, 2017

TIME: 9:00 am – 12:00 pm EST

LOCATION: CASE Offices, 805 Brook Street, Building 4 – CERC, Rocky Hill (see directions

attached)

AGENDA: *See Attached*

TELECONFERENCE IS AVAILABLE:
Dial: 866-740-1260
Access: 5272161#

Best regards -

Terri Clark
Associate Director
Connecticut Academy of Science and Engineering
805 Brook Street, Building 4-CERC
Rocky Hill, CT 06067-3405
860/571-7143
mailto:tclark@ctcase.org

From: Bender, Sean (POL)
To: Slattery, John (POL)
Subject: Fw: ALPR accounts
Date: Thursday, March 23, 2017 3:43:39 PM
Attachments: image001.png
image004.png
BOSS_3.2x_User_Manual_final.pdf

From: Bender, Sean (POL)
Sent: Monday, November 21, 2016 11:16 AM
To: Jorge, Lucas (POL)
Subject: Fw: ALPR accounts

Sir,

Here are the instructions for setting up 3M (LPR).

You should be able to access it through the M-Drive in the folder called "SA Client 3.2.0", just look for the application with the little red "3M" icon and then follow the instructions below to set it up.

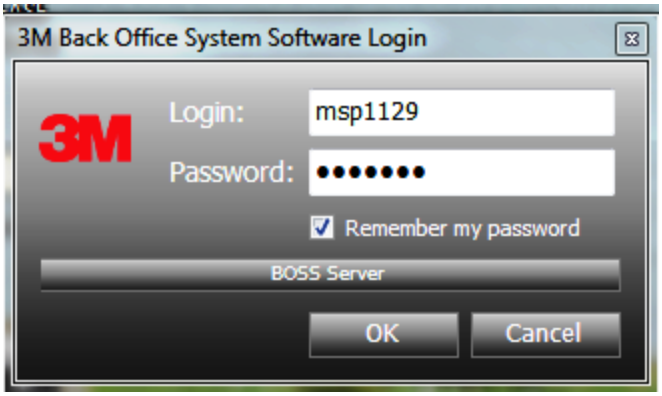
Hope this helps! If you have any trouble, give us a call.

Sean Bender
Massachusetts State Police
Commonwealth Fusion Center
124 Acton Street
Maynard, MA 01754
978-451-3700 (phone)
978-451-3707 (fax)

From: Griffin, Daniel (POL)
Sent: Friday, September 2, 2016 12:24 PM
To: Bender, Sean (POL); Bois, Marcy (POL); Boyle, Christopher (POL); Brooks, Robert (POL); Crowley, Timothy (POL); Duggan, James M (POL); Favale, Matthew (POL); Ferrazzani, Kurt (POL); Foley, Kristine (POL); Foster, John (POL); Huchowski, James (POL); Huchowski, kerra (POL); Jorge, Lucas (POL); Neville, Chris; Nystrom, Lindsey (POL); O'Leary, Sarah (POL); Panacopoulos, Laurie (POL); Pirrotta, Melissa (POL); Porter, Rebekkah (POL); Sarrouf, Thomas (POL); Slattery, John (POL); Thibault, Amy (POL); Upton, Paul (POL); Wilczynski, Kristin (POL)
Cc: Mason, Christopher (POL); Egnitz, Brian (POL)
Subject: ALPR accounts

Good Afternoon,

The 3M ALPR software has been placed on the server at the fusion center. Accounts have been set up for all addressed. The default password is “fusion” all lower case. Your log in is either your civilian number ex-C1474 or your SP id ex-msp2710.
Initial log in-
When you first log in some changes (port & IP address) need to be changed. These settings should remain once changed on initial log in.
The log in screen should look like this: (Login/Password will be blank)



Fill in your user name and password then click on the “Boss Server” bar directly below:



Please configure the server & port with these settings and hit “ok”
This should get you into the system.
I have attached an electronic copy of the user manual as well. Please feel free to contact me w/ any questions or concerns.

I will be in touch with respect to training.

Respectfully,

Lieutenant Daniel J. Griffin 1129
Massachusetts State Police
Traffic Programs Section
General Headquarters
470 Worcester Rd
Framingham, Ma. 01702
508-988-7404
daniel.griffin@massmail.state.ma.us



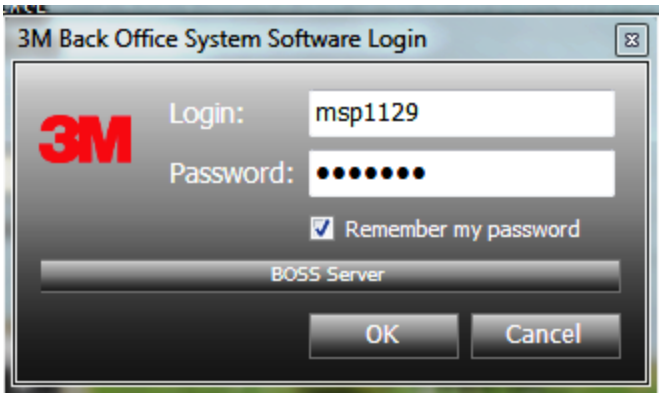
From:	Bender, Sean (POL)
To:	Sojka, Robert (POL)
Subject:	Fw: ALPR accounts
Date:	Thursday, March 2, 2017 3:58:32 PM
Attachments:	image001.png image004.png BOSS_3.2x_User_Manual_final.pdf

---

From: Griffin, Daniel (POL)
Sent: Friday, September 2, 2016 12:24 PM
To: Bender, Sean (POL); Bois, Marcy (POL); Boyle, Christopher (POL); Brooks, Robert (POL); Crowley, Timothy (POL); Duggan, James M (POL); Favale, Matthew (POL); Ferrazzani, Kurt (POL); Foley, Kristine (POL); Foster, John (POL); Huchowski, James (POL); Huchowski, kerra (POL); Jorge, Lucas (POL); Neville, Chris; Nystrom, Lindsey (POL); O'Leary, Sarah (POL); Panacopoulos, Laurie (POL); Pirrotta, Melissa (POL); Porter, Rebekkah (POL); Sarrouf, Thomas (POL); Slattery, John (POL); Thibault, Amy (POL); Upton, Paul (POL); Wilczynski, Kristin (POL)
Cc: Mason, Christopher (POL); Egnitz, Brian (POL)
Subject: ALPR accounts

Good Afternoon,

The 3M ALPR software has been placed on the server at the fusion center. Accounts have been set up for all adressed. The default password is “fusion” all lower case. Your log in is either your civilian number ex-C1474 or your SP id ex-msp2710.
Initial log in-
When you first log in some changes (port & IP address) need to be changed. These settings should remain once changed on initial log in.
The log in screen should look like this: (Login/Password will be blank)



Fill in your user name and password then click on the “Boss Server” bar directly below:



Please configure the server & port with these settings and hit “ok”
This should get you into the system.
I have attached an electronic copy of the user manual as well. Please feel free to contact me w/ any questions or concerns.

I will be in touch with respect to training.

Respectfully,

Lieutenant Daniel J. Griffin 1129
Massachusetts State Police
Traffic Programs Section
General Headquarters
470 Worcester Rd
Framingham, Ma. 01702
508-988-7404
daniel.griffin@massmail.state.ma.us

From: Huchowski, James (POL)
To: Slattery, John (POL)
Subject: Fw: ALPR accounts
Date: Thursday, February 9, 2017 11:05:04 PM
Attachments: BOSS_3.2x_User_Manual_final.pdf
ATT00001.htm

---

here is the LPR email for access.

From: Huchowski, James (POL)
Sent: Thursday, January 12, 2017 12:09 AM
To: James Huchowski
Subject: Fwd: ALPR accounts

Sent from my iPhone

Begin forwarded message:

> **From:** "Griffin, Daniel (POL)" <daniel.griffin@MassMail.State.MA.US>
> **To:** "Bender, Sean (POL)" <sean.bender@MassMail.State.MA.US>, "Bois, Marcy (POL)" <marcy.bois@MassMail.State.MA.US>, "Boyle, Christopher (POL)" <christopher.boyle@MassMail.State.MA.US>, "Brooks, Robert (POL)" <Robert.Brooks@MassMail.State.MA.US>, "Crowley, Timothy (POL)" <timothy.crowley@MassMail.State.MA.US>, "Duggan, James M (POL)" <james.duggan2@MassMail.State.MA.US>, "Favale, Matthew (POL)" <matthew.favale@MassMail.State.MA.US>, "Ferrazzani, Kurt (POL)" <kurt.ferrazzani@MassMail.State.MA.US>, "Foley, Kristine (POL)" <kristine.foley@MassMail.State.MA.US>, "Foster, John (POL)" <john.foster@MassMail.State.MA.US>, "Huchowski, James (POL)" <james.huchowski@MassMail.State.MA.US>, "Huchowski, kerra (POL)" <kerra.huchowski@MassMail.State.MA.US>, "Jorge, Lucas (POL)" <lucas.jorge@MassMail.State.MA.US>, "Neville, Chris" <cneville@wpd.org>, "Nystrom, Lindsey (POL)" <lindsey.nystrom@MassMail.State.MA.US>, "O'Leary, Sarah (POL)" <sj.oleary@MassMail.State.MA.US>, "Panacopoulos, Laurie (POL)" <laurie.panacopoulos@MassMail.State.MA.US>, "Pirrotta, Melissa (POL)" <melissa.pirrotta@MassMail.State.MA.US>, "Porter, Rebekkah (POL)" <rebekkah.porter@MassMail.State.MA.US>, "Sarrouf, Thomas (POL)" <thomas.sarrouf@MassMail.State.MA.US>, "Slattery, John (POL)" <john.slattery@MassMail.State.MA.US>, "Thibault, Amy (POL)" <amy.thibault@MassMail.State.MA.US>, "Upton, Paul (POL)" <paul.upton@MassMail.State.MA.US>, "Wilczynski, Kristin (POL)"

<kristin.wilczynski@MassMail.State.MA.US>
Cc: "Mason, Christopher (POL)" <chris.mason@MassMail.State.MA.US>, "Egnitz, Brian (POL)" <brian.egnitz@MassMail.State.MA.US>
Subject: ALPR accounts

Good Afternoon,

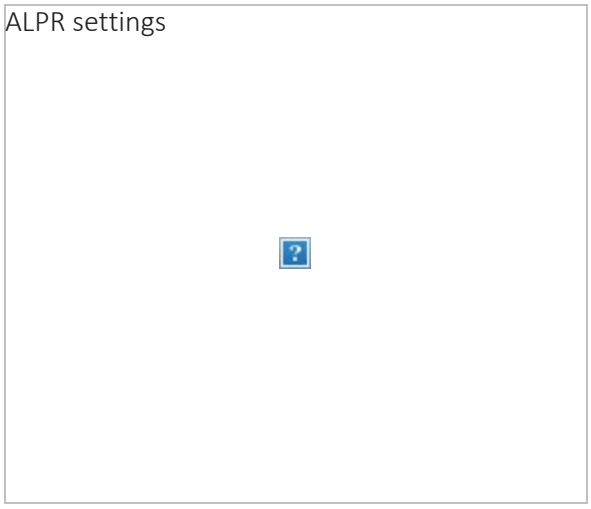
The 3M ALPR software has been placed on the server at the fusion center. Accounts have been set up for all adressed. The default password is “fusion” all lower case. Your log in is either your civilian number ex-C1474 or your SP id ex-msp2710.
Initial log in-
When you first log in some changes (port & IP address) need to be changed. These settings should remain once changed on initial log in.
The log in screen should look like this: (Login/Password will be blank)

log in screen



Fill in your user name and password then click on the “Boss Server” bar directly below:

ALPR settings



Please configure the server & port with these settings and hit “ok”
This should get you into the system.
I have attached an electronic copy of the user manual as well. Please feel free to contact me w/ any questions or concerns.

I will be in touch with respect to training.

Respectfully,

Lieutenant Daniel J. Griffin 1129
Massachusetts State Police
Traffic Programs Section
General Headquarters
470 Worcester Rd
Framingham, Ma. 01702
508-988-7404
daniel.griffin@massmail.state.ma.us



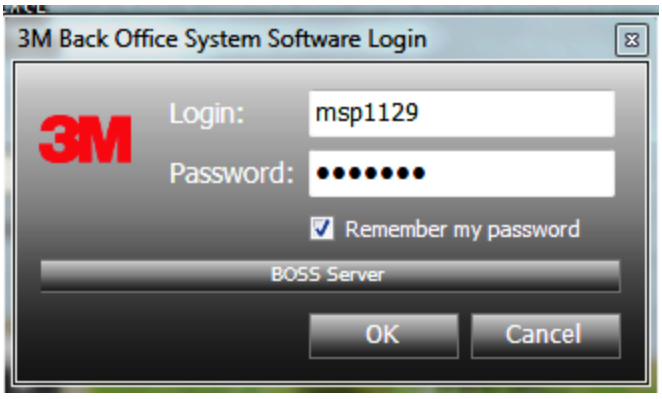
From:	Bender, Sean (POL)
To:	Huchowski, kerra (POL)
Subject:	Fw: ALPR accounts
Date:	Thursday, March 30, 2017 10:25:13 AM
Attachments:	image001.png image004.png BOSS_3.2x_User_Manual_final.pdf

---

From: Griffin, Daniel (POL)
Sent: Friday, September 2, 2016 12:24 PM
To: Bender, Sean (POL); Bois, Marcy (POL); Boyle, Christopher (POL); Brooks, Robert (POL); Crowley, Timothy (POL); Duggan, James M (POL); Favale, Matthew (POL); Ferrazzani, Kurt (POL); Foley, Kristine (POL); Foster, John (POL); Huchowski, James (POL); Huchowski, kerra (POL); Jorge, Lucas (POL); Neville, Chris; Nystrom, Lindsey (POL); O'Leary, Sarah (POL); Panacopoulos, Laurie (POL); Pirrotta, Melissa (POL); Porter, Rebekkah (POL); Sarrouf, Thomas (POL); Slattery, John (POL); Thibault, Amy (POL); Upton, Paul (POL); Wilczynski, Kristin (POL)
Cc: Mason, Christopher (POL); Egnitz, Brian (POL)
Subject: ALPR accounts

Good Afternoon,

The 3M ALPR software has been placed on the server at the fusion center. Accounts have been set up for all adressed. The default password is “fusion” all lower case. Your log in is either your civilian number ex-C1474 or your SP id ex-msp2710.
Initial log in-
When you first log in some changes (port & IP address) need to be changed. These settings should remain once changed on initial log in.
The log in screen should look like this: (Login/Password will be blank)



Fill in your user name and password then click on the “Boss Server” bar directly below:



Please configure the server & port with these settings and hit “ok”
This should get you into the system.
I have attached an electronic copy of the user manual as well. Please feel free to contact me w/ any questions or concerns.

I will be in touch with respect to training.

Respectfully,

Lieutenant Daniel J. Griffin 1129
Massachusetts State Police
Traffic Programs Section
General Headquarters
470 Worcester Rd
Framingham, Ma. 01702
508-988-7404
daniel.griffin@massmail.state.ma.us

From: Egnitz, Brian (POL)
To: Thibault, Amy (POL)
Subject: FW: ALPR Quote
Date: Friday, April 28, 2017 7:42:00 AM
Attachments: Est_QACS172053_from_Access_Control_Systems_7204.pdf
DELLR730_APP_30000007937101.pdf
DELLR730_DB_30000007929391.pdf
MSP DIRECT_P492 Fixed Camera + Plate Alert Software.pdf
Plate Alert brochure.pdf
MHQ Quote per Contract #SP16-MSPVEH-F80 - Rev 1.pdf

These were the last quotes we got

	Type	Quantity	Cost	Sub Total
	Truck	[redacted]		$ 58,256.00
	LPR			$ 357,570.00
	Trailer			$ 521,550.00
Fixed/Reoccurring Costs	Server upgrade			$ 29,365.77
Fixed/Reoccurring Costs	Software update			$ 62,040.00
Fixed/Reoccurring Costs	Verizon			$ 18,000.00
				$ 1,046,781.77

From: Egnitz, Brian (POL)
Sent: Friday, March 24, 2017 2:14 PM
To: Mason, Christopher (POL)
Cc: Quinn, Dermot (POL)
Subject: ALPR Quote

Please find the attached quotes for 30 LPRs and 30 Solar Trailers. I'm still waiting on a quote for 2 4x4 trucks.

Total LPR $419,610
Total Trailer $508,400.00
Server Upgrade $29,365.77
Total Cost $957,357.77 + 2 4x4 trucks $ TBD

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
978-451-3710 (Maynard)
508-988-7216 (GHQ)

From: Egnitz, Brian (POL)
To: Babbin, Timothy (MGC)
Subject: FW: ALPR Readers
Date: Monday, July 31, 2017 10:29:00 AM
Attachments: image005.png
image007.png
image006.png
image008.png
BOSS_3.2x_User_Manual_final.pdf
ALPR Hot Lists Job Aid.pdf

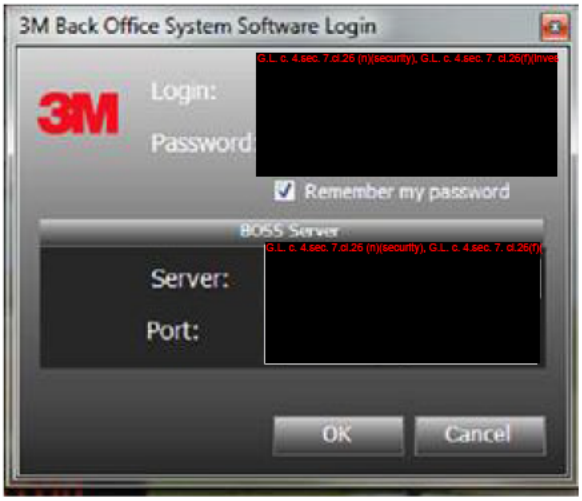
Camera name is 5495201_Rt1@Plainri

Hotlist is called "Plainridge"

If you need a plate added, just email fusion and ask them to add to the "Plainridge" list. Also include which emails you want to have them go to. fusion@MassMail.State.MA.US

This has already been done.

Configure as below (under BOSS Server)



Software can be downloaded here (already done)

https://170.154.225.38/learn

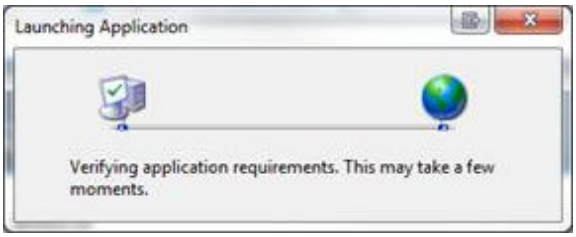
PIPS BOSS Procedure

Installing the BOSS.UI Client

From a browser, go to the below URL and Click "Log into BOSS" to begin the setup process:
http://170.154.225.78:9988/publish.htm



An application verification will take place and if needed, .net will be installed.



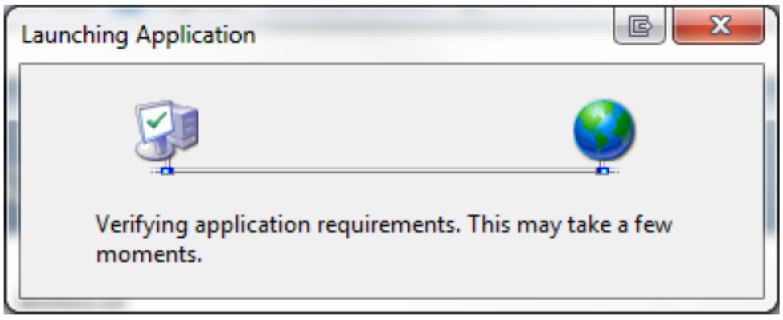
After .Net, the BOSS application will be installed.



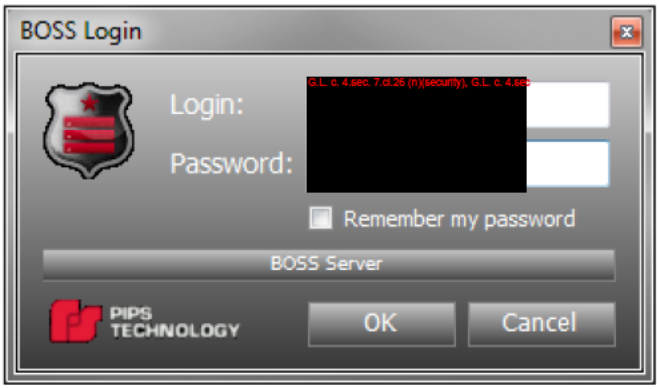
The BOSS.UI icon will be placed on your desktop:



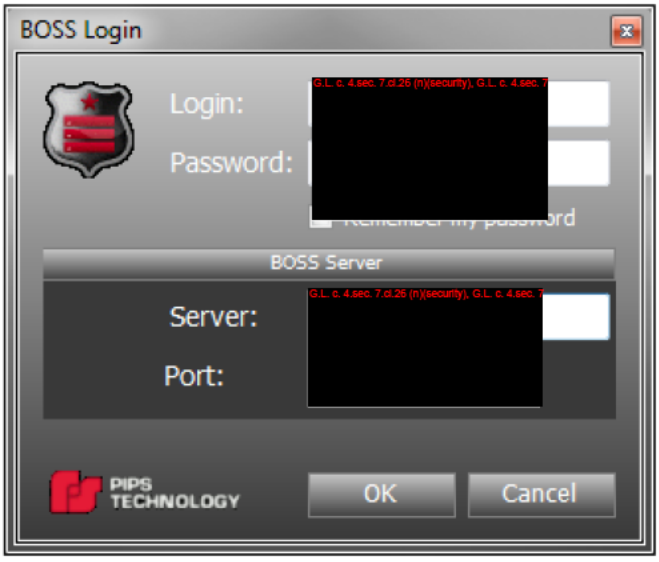
Double click to launch the application. The .Net verification will take place quickly:



The application log-in box will appear, enter your credentials but do NOT click OK yet, see next step:



Click the BOSS Server button so that the correct server information can be entered, 170.154.225.78 and change the port to 8443 (Note-this will need to be changed EVERY time), then click "OK":



The main page will appear:



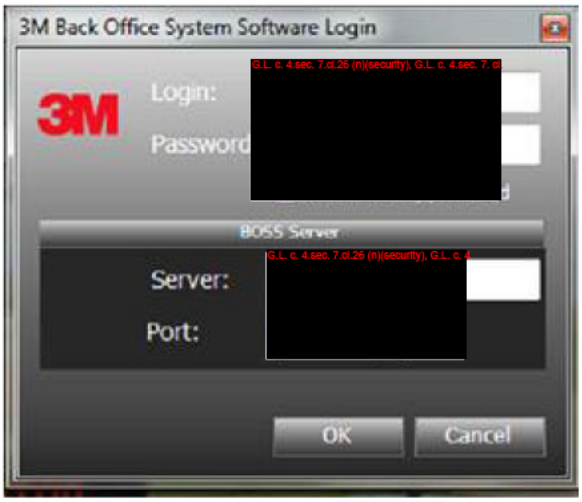
Shannon Clarke | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Infrastructure and Network Services
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea MA 02150
p. 617.660.4620 | f. 617.884.4601
shannon.clarke@state.ma.us I
http://www.mass.gov/eopss

From: Egnitz, Brian (POL)
To: Morrissette, Brock A (POL)
Subject: FW: ALPR Readers
Date: Wednesday, August 9, 2017 2:12:00 PM
Attachments: image005.png
image007.png
image006.png
image008.png
BOSS_3.2x_User_Manual_final.pdf
ALPR Hot Lists Job Aid.pdf

User name is msp[id] and Pass@[ID]

Camera name is SIGNBOARD_AcushnetNB

Configure as below (under BOSS Server)



Software can be downloaded here

https://170.154.225.38/learn

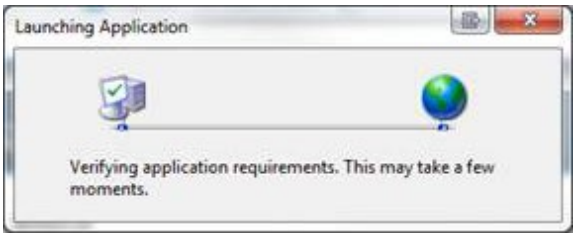
PIPS BOSS Procedure

Installing the BOSS.UI Client

From a browser, go to the below URL and Click "Log into BOSS" to begin the setup process:
http://170.154.225.78:9988/publish.htm



An application verification will take place and if needed, .net will be installed.



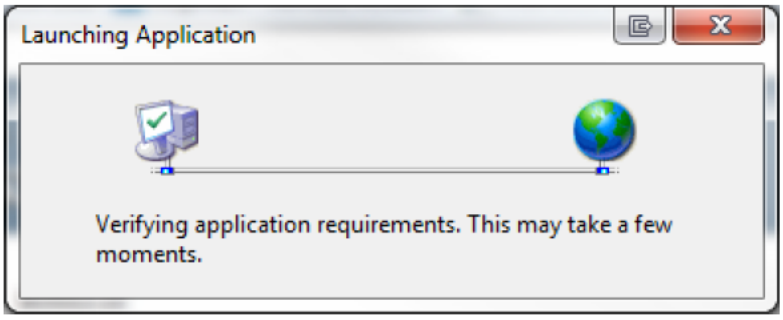
After .Net, the BOSS application will be installed.



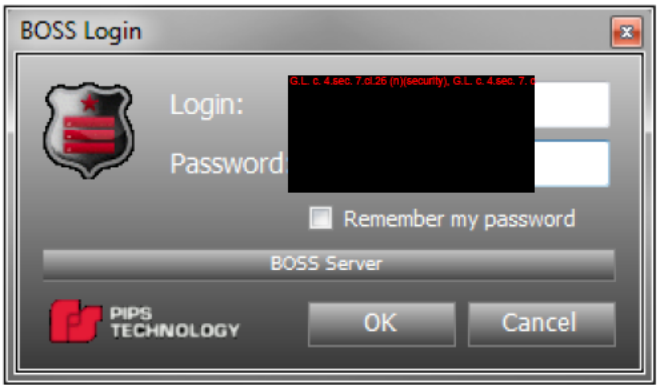
The BOSS.UI icon will be placed on your desktop:



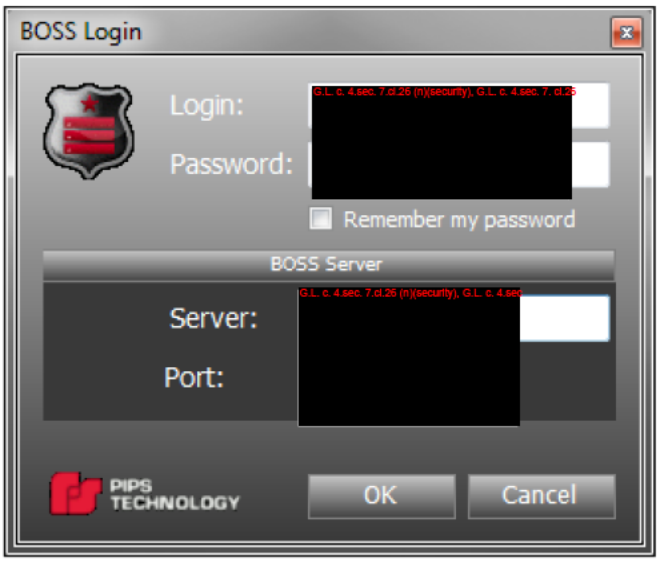
Double click to launch the application. The .Net verification will take place quickly:



The application log-in box will appear, enter your credentials but do NOT click OK yet, see next step:



Click the BOSS Server button so that the correct server information can be entered, 170.154.225.78 and change the port to 8443 (Note-this will need to be changed EVERY time), then click "OK":



The main page will appear:


File Help
Look For:
In:
Reads
Find
Clear
Welcome to BOSS3, Sean Hughes
Reads:
2875
Hits:
0
Misreads:
0
Total Reads:
2875
Total Hits:
0
BOSS
PIPS
TECHNOLOGY

From: Mitchell, Timothy (EPS)
To: mroth@neology.net
Cc: Egnitz, Brian (POL)
Subject: FW: Boss puge
Date: Tuesday, October 31, 2017 12:36:53 PM
Attachments: mroth.txt
EOPSS_PC_Cert_and_Client_InstallV3.2.docx

Michael
We already had a VPN provisioned for you so I have issued a new certificate under that profile. Cert enrollment along with client and cert installation instructions are attached. You should already have access to the server once you get this installed.

Let me know if you need the password as well.
Thanks

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

From: Egnitz, Brian (POL)
Sent: Monday, October 30, 2017 5:28 PM
To: Mitchell, Timothy (EPS)
Subject: Fwd: Boss puge

Begin forwarded message:

> **From:** Michael Roth <mroth@neology.net>
> **Date:** October 30, 2017 at 2:22:09 PM EDT
> **To:** "brian.egnitz@MassMail.State.MA.US" <brian.egnitz@massmail.state.ma.us>
> **Cc:** John Tedona CW <jtedona@mmm.com>
> **Subject: Boss puge**
>
> Brian, i can take a look on friday moring around 9:30am. Would be possable for you to get me remote vpn access setup by then?

Michael B. Roth
Application Engineer
C: 513 767 7610
mroth@neology.net
www.neology.net
ALPR Support Line: 877 777 3571 | alprsupportus@mmm.com

From: Egnitz, Brian (POL)
To: Quinn, Dermot (POL); Mason, Christopher (POL)
Cc: Range, Scott (POL)
Subject: FW: Bourne Bridge LPR Request
Date: Thursday, December 7, 2017 11:37:43 AM
Attachments: RE Boss puge.msg
RE Purge.msg
Re Purge.msg
Purge.msg
RE BOSS ALPR Storage.msg
Re BOSS ALPR Storage.msg
RE BOSS ALPR Storage.msg
BOSS ALPR Storage.msg
FW SR# S1575305 LOGGED BOSS Crash again.msg
LPR Stats for storage.msg
EOTSS - Meeting Notes.msg

FYI –

I suspect this was the time period where BOSS had crashed due to a lack of disc space. Tpr. Doherty and I were at Norwood PD on 11/27 and after the meeting we received notification that the system was down. I then worked to add capacity and begin to truncate the log myself.

We have notified EOPSS a number of times as seen in the attached emails, however this continues to be a problem. I have double checked this in SQL and it looks like the server may have filled up around 11/25/17 16:17 hours and was restored by 11/27/17 around 11 AM. If my suspicion is correct, this would be the second Homicide investigation were potentially valuable ALPR intelligence would have been lost due to an issue that could have been easily mitigated.

-Brian

From: Commonwealth Fusion Center (POL)
Sent: Thursday, December 07, 2017 10:53 AM
To: Egnitz, Brian (POL)
Cc: Boyle, Christopher (POL); Archive Fusion
Subject: Bourne Bridge LPR Request

Good Morning Brian –

Per Sgt. Boyle, can you try and run MA Commercial J26941 through the Bourne Bridge plate readers and see what comes up?

Could we also run a broad query for all the hits on the Bourne Bridge for 11/26/2017 between 2330 & 0030 the following morning? We tried to run the same here, but it was returning no results. I may have been entering the query incorrectly, but we ran a test query for 12/7/2017 between 1000 and 1010 and turned up over 500 hits in that 10 minute block…

I can't imagine an hour block on the Bourne bridge returns no reads unless the server or device was down or something…

Any advice/help would be much appreciated so we can make sure we're able to do this ourselves in the future. Thanks!

Respectfully,

Sean Bender
Intelligence Analyst
Massachusetts State Police
S.P.E.A.R Center
470 Worcester Rd.
Framingham, MA 01702
508-820-2233
Sean.Bender@massmail.state.ma.us

From:	Thibault, Amy (POL)
To:	Mason, Christopher (POL)
Subject:	FW: CICC Release of the License Plate Reader (LPR) Policy Development Template for Use in Intelligence and Investigative Activities
Date:	Thursday, February 16, 2017 11:15:03 AM
Attachments:	image001.png LPR Policy Template FINAL 2-7-17.pdf

From: LEIU [mailto:LEIU@doj.ca.gov]
Sent: Wednesday, February 08, 2017 6:44 PM
To: LEIU
Subject: CICC Release of the License Plate Reader (LPR) Policy Development Template for Use in Intelligence and Investigative Activities

Dear LEIU Members,

Through a collaborative partnership among the associations represented on the Criminal Intelligence Coordinating Council (CICC)—including LEIU--the U.S. Department of Homeland Security, the Bureau of Justice Assistance, and numerous federal, state, and local partners, the CICC has released the ***License Plate Reader Policy Development Template for Use in Intelligence and Investigative Activities*** (LPR Policy Template). This policy guidance resource is designed specifically for law enforcement entities and fusion centers to assist their efforts developing and implementing comprehensive privacy, civil rights, and civil liberties policies regarding the use of automated license plate readers (ALPRs or LPRs) in intelligence and investigative activities. Justice entities are turning to LPR technology to help solve crimes, recover abducted children, detect trafficking rings, and support terrorism investigations. However, when considering or implementing an LPR program, individual privacy, civil rights, and civil liberties must also be vigorously protected. Justice entities should therefore develop appropriate policies and procedures to guard against possible errors and other potential problems. Such proactive work supports and enhances the justice entity's ability to fulfill its mission while also protecting the privacy, civil rights, and civil liberties of community members. Through the effective and responsible use of LPR technology, agencies strengthen trust and public confidence.

Developed by state, local, and federal law enforcement practitioners with LPR expertise and privacy subject-matter experts (SMEs), the provisions of the LPR Policy Template are intended to be incorporated into agency operational policies and day-to-day operations. Each section represents a fundamental component of a comprehensive policy that includes baseline provisions on LPR information collection; information quality; access and disclosure; redress; security, retention, and destruction; accountability and enforcement; and training. Sample language is provided for each recommended provision, as well as appendices that contain a glossary of terms and definitions, citations to federal and case law, and a draft model policy.

Please distribute this to members in your agency who will most benefit. This document has also been posted on the LEIU Secure Portal.

Sincerely,

Bob Morehouse, Executive Director
Association of Law Enforcement Intelligence Units (LEIU)
Work Phone: (916) 263-1178
Cell Phone: (916) 704-4949
Bob.morehouse@doj.ca.gov



Association of
Law Enforcement Intelligence Units
www.leiu.org

CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.

From:	Sullivan, Quinn
To:	Duggan, James M (POL); Mason, Christopher (POL); Range, Scott (POL); Sojka, Robert (POL); Thibault, Amy (POL)
Subject:	FW: CICC Release of the License Plate Reader (LPR) Policy Development Template for Use in Intelligence and Investigative Activities
Date:	Wednesday, February 8, 2017 7:32:07 PM
Attachments:	LPR Policy Template FINAL 2-7-17.pdf

FYI

From: SLTT Partner Engagement
Sent: Wednesday, February 8, 2017 8:36 AM
To: RISS Center <RISSCenter@hq.dhs.gov>; Fusion Center Directors <FusionCenterDirectors@hq.dhs.gov>; HIDTA Directors <HIDTA_Directors@hq.dhs.gov>; HIDTA ISC Managers <HIDTA-ISC-Managers@hq.dhs.gov>; SLIC <SLIC@hq.dhs.gov>; SL Partners <SLPARTNERS@HQ.DHS.GOV>
Cc: Field Ops (ALL) <FieldOpsAll@hq.dhs.gov>; OSLLE <OSLLE@HQ.DHS.GOV>; DHS.IGA <dhs.iga@hq.dhs.gov>
Subject: CICC Release of the License Plate Reader (LPR) Policy Development Template for Use in Intelligence and Investigative Activities

Partners–

Through a collaborative partnership among the associations represented on the Criminal Intelligence Coordinating Council (CICC), the U.S. Department of Homeland Security, the Bureau of Justice Assistance, and numerous federal, state, and local partners, we are pleased to announce the official release of the ***License Plate Reader Policy Development Template for Use in Intelligence and Investigative Activities*** (LPR Policy Template). This policy guidance resource is designed specifically for law enforcement entities and fusion centers to assist their efforts developing and implementing comprehensive privacy, civil rights, and civil liberties policies regarding the use of automated license plate readers (ALPRs or LPRs) in intelligence and investigative activities. Justice entities are turning to LPR technology to help solve crimes, recover abducted children, detect trafficking rings, and support terrorism investigations. However, when considering or implementing an LPR program, individual privacy, civil rights, and civil liberties must also be vigorously protected. Justice entities should therefore develop appropriate policies and procedures to guard against possible errors and other potential problems. Such proactive work supports and enhances the justice entity's ability to fulfill its mission while also protecting the privacy, civil rights, and civil liberties of community members. Through the effective and responsible use of LPR technology, agencies strengthen trust and public confidence.

Developed by state, local, and federal law enforcement practitioners with LPR expertise and privacy subject-matter experts (SMEs), the provisions of the LPR Policy Template are intended to be incorporated into agency operational policies and day-to-day operations. Each section

represents a fundamental component of a comprehensive policy that includes baseline provisions on LPR information collection; information quality; access and disclosure; redress; security, retention, and destruction; accountability and enforcement; and training. Sample language is provided for each recommended provision, as well as appendices that contain a glossary of terms and definitions, citations to federal and case law, and a draft model policy.

Please also distribute this to your association and organization members.

Thank you,

Mr. Vernon Keenan
Chair, Criminal Intelligence Coordinating Council
Director, Georgia Bureau of Investigation

Deputy Chief Mike Downing
Vice-chair, Criminal Intelligence Coordinating Council
Los Angeles Police Department

From:	Panacopoulos, Laurie (POL)
To:	Thibault, Amy (POL)
Subject:	FW: CICC Release of the License Plate Reader (LPR) Policy Development Template for Use in Intelligence and Investigative Activities
Date:	Thursday, March 9, 2017 10:24:00 AM
Attachments:	image001.png LPR Policy Template FINAL 2-7-17.pdf

Do you think anyone would be interested in this? What about Lt Dan Griffin in Traffic Programs?

From: LEIU [mailto:LEIU@doj.ca.gov]
Sent: Wednesday, February 08, 2017 6:44 PM
To: LEIU
Subject: CICC Release of the License Plate Reader (LPR) Policy Development Template for Use in Intelligence and Investigative Activities

Dear LEIU Members,

Through a collaborative partnership among the associations represented on the Criminal Intelligence Coordinating Council (CICC)—including LEIU--the U.S. Department of Homeland Security, the Bureau of Justice Assistance, and numerous federal, state, and local partners, the CICC has released the ***License Plate Reader Policy Development Template for Use in Intelligence and Investigative Activities*** (LPR Policy Template). This policy guidance resource is designed specifically for law enforcement entities and fusion centers to assist their efforts developing and implementing comprehensive privacy, civil rights, and civil liberties policies regarding the use of automated license plate readers (ALPRs or LPRs) in intelligence and investigative activities. Justice entities are turning to LPR technology to help solve crimes, recover abducted children, detect trafficking rings, and support terrorism investigations. However, when considering or implementing an LPR program, individual privacy, civil rights, and civil liberties must also be vigorously protected. Justice entities should therefore develop appropriate policies and procedures to guard against possible errors and other potential problems. Such proactive work supports and enhances the justice entity's ability to fulfill its mission while also protecting the privacy, civil rights, and civil liberties of community members. Through the effective and responsible use of LPR technology, agencies strengthen trust and public confidence.

Developed by state, local, and federal law enforcement practitioners with LPR expertise and privacy subject-matter experts (SMEs), the provisions of the LPR Policy Template are intended to be incorporated into agency operational policies and day-to-day operations. Each section represents a fundamental component of a comprehensive policy that includes baseline provisions on LPR information collection; information quality; access and disclosure; redress; security, retention, and destruction; accountability and enforcement; and training. Sample language is provided for each recommended provision, as well as appendices that contain a glossary of terms and definitions, citations to federal and case law, and a draft model policy.

Please distribute this to members in your agency who will most benefit. This document has also been posted on the LEIU Secure Portal.

Sincerely,

Bob Morehouse, Executive Director
Association of Law Enforcement Intelligence Units (LEIU)
Work Phone: (916) 263-1178
Cell Phone: (916) 704-4949
Bob.morehouse@doj.ca.gov



Association of
Law Enforcement Intelligence Units
www.leiu.org

CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.

From:	Egnitz, Brian (POL)
To:	Thibault, Amy (POL)
Subject:	FW: CopLink
Date:	Monday, September 25, 2017 10:37:00 AM

From: Egnitz, Brian (POL)
Sent: Monday, July 17, 2017 11:27 AM
To: 'Pouliot, Peter P 1SG USARMY NG MAARNG (US)'
Subject: RE: CopLink

I spoke to IBM regarding contract info, let me know when we can set up a meeting to discuss.

From: Egnitz, Brian (POL)
Sent: Friday, June 30, 2017 7:49 AM
To: Pouliot, Peter P 1SG USARMY NG MAARNG (US)
Subject: RE: CopLink

Hi Pete,

How are we making out on funding?

-Brian

From: Egnitz, Brian (POL)
Sent: Wednesday, May 10, 2017 11:32 AM
To: 'peter.p.pouliot.mil@mail.mil'
Cc: Quinn, Dermot (POL); Mason, Christopher (POL); Sojka, Robert (POL)
Subject: CopLink

Hi Pete,

Per your request, here are some of the CopLink projects that we need funded.

Thanks, Brian

CopLink Enhancements

Project Description:

The Commonwealth of Massachusetts's Fusion Center hosts IBM i2 COPLINK for Local, State and Federal law enforcement agencies. IBM i2 COPLINK is police investigation software that consolidates data from many sources, aids collaboration and helps generate tactical leads quickly. CopLink is used to search record management systems, registry data and criminal history records to solve various crime, such as Homicides, Drug Trafficking and Bank Robberies. This tool provides advanced analytics to law enforcement, data exchange and interoperability to improve connectivity between information sharing systems.

Scope of Work

1. Map the Boston Police Departments Record Management System into CopLink ($28,300)
2. Map the MBTA (Massachusetts Bay Transit Authority) Police Records System into CopLink. ($18,800)
3. Map Lawrence Police Department Record Management System into CopLink (est. $25,000)
4. Map Board of Probation data into CopLink ($22,400)
5. Enhance CopLink to show RMV (Registry of Motor Vehicles) driver's license photos inside of the CopLink software ($63,760)
6. Map the States Automated License Plate Reader Database into CopLink (est. $30,000)
7. Map the States Electronic Citation Database (Civil Motor Vehicle Citation) ($19,850)

Definitions:

A records management system (RMS) is "an agency-wide system that provides for the storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, or files pertaining to law enforcement operations. RMS covers the entire life span of records development—from the initial generation to its completion. An effective RMS allows single entry of data, while supporting multiple reporting mechanisms." (This definition is taken from both the Bureau of Justice Assistance's Standard Functional Specifications for Law Enforcement Records Management Systems and the International Association of Chiefs of Police [IACP]/Department of Justices' Community Oriented Policing Services [COPS] Technology Technical Assistance Program's Records Management Systems documents.)

"Records" are the information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business. The International Council on Archives (ICA) Committee on Electronic Records defines a record as, "recorded information produced or received in the initiation, conduct or completion of an institutional or individual activity and that comprises content, context and structure sufficient to provide evidence of the activity."

BOP database contains Criminal Offender Record Information, which consists of records and data in any communicable form compiled by a Massachusetts criminal justice agency about an identifiable individual that relate to:

- Nature or disposition of a criminal charge,
- An arrest,
- A pre-trial proceeding,
- Other judicial proceedings,
- Sentencing,
- Incarceration,
- Rehabilitation,

- Release

Automated License Plate Recognition (ALPR) is a technology that uses optical character recognition (OCR) to automatically read license plate characters.

There are two types of ALPR: stationary, which uses infrared (IR) cameras at high fixed points, and mobile, which uses vehicle-mounted IR cameras.

Stationary cameras can be mounted on signs, street lights, highway overpasses or buildings as a cost-effective way to monitor moving and parked vehicles twenty-four hours a day. Camera software is able to identify the pixel patterns that make up a license plate and translate the letters and numbers on the plate to a digital format. The plate data is then sent to a database where it is compared in real-time to a list of plate numbers that belong to "vehicles of interest". If the system detects a match, it sends an alert to the dispatcher or other designated personnel.

Mobile ALPR software suites use multiple cameras mounted on a vehicle. As the vehicle moves, it photographs license plates and transmits plate data to a database. The database may be a national database or it may be created at the local level and downloaded into the vehicle's onboard computer at the beginning of each shift. If the system detects a match, the officer receives an alert on his computer. A mobile ALPR can read up to 1,000 plates per hour and cover two or more lanes of traffic at once.

Automated License Plate Recognition has many uses including:
•Recovering stolen cars.
•Identifying drivers with an open warrant for arrest.
•Catching speeders by comparing the average time it takes to get from stationary camera A to stationary camera B.
•Determining what cars do and do not belong in a parking garage.
•Expediting parking by eliminating the need for human confirmation of parking passes.

ALPR is known by several other names, including Automatic Number Plate Recognition (ANPR), Automatic Vehicle Identification (AVI), Car Plate Recognition (CPR), License Plate Recognition (LPR), and Lecture Automatique de Plaques d'Immatriculation (LAPI).

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7216 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

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

From: Taylor, Rita (POL)
To: Sojka, Robert (POL)
Subject: FW: FJAGHEOP16 5TH DIVISION
Date: Wednesday, November 29, 2017 12:56:00 PM
Attachments: ISA FJAGHEOP16 5TH DIVISION ALPR purchases - Attachment A.doc

Hi we made a few changes in the equipment section. We prefer to not list it all out in case a particular model/brand is not available. Please review and if you are agreement please initial all pages of the terms and conditions and return to me.

Thanks

Rita

From: Taylor, Rita (POL)
Sent: Wednesday, November 29, 2017 11:24 AM
To: Rivera Morgan, Awilda (POL)
Subject: FW: FJAGHEOP16 5TH DIVISION

Can you review the attachment A.

Thanks

From: Sojka, Robert (POL)
Sent: Wednesday, November 29, 2017 11:04 AM
To: Taylor, Rita (POL)
Subject: RE: FJAGHEOP16 5TH DIVISION

Can you give this a quick look to be sure it is acceptable?

-Bob

From: Taylor, Rita (POL)
Sent: Tuesday, November 28, 2017 4:15 PM
To: Sojka, Robert (POL)
Subject: FJAGHEOP16 5TH DIVISION
Importance: High

Hi , could you please complete the attachment A initial each page of the ISA , and complete the Project Manager Responsibilities form.

Please let me know if you have any questions.

Thanks

Rita
Rita Taylor

Grant Administrator/Acting Payroll Director
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2151
Rita.Taylor@State.Ma.US

From: Maloney, Colleen (OGR)
Sent: Tuesday, November 28, 2017 2:33 PM
To: Taylor, Rita (POL)
Subject:
Importance: High

Hi Rita,

I want to make sure I get these to the right person, are you going to be handling the grant info for MSPs new 5th division? If so attached are the ISA documents, could you please get them signed and sent back?

Thanks!
Colleen

Colleen Maloney
Justice and Prevention
Executive Office of Public Safety and Security/OGR
Ten Park Plaza, Suite 3720
Boston, MA 02116
617-725-3316

From: Taylor, Rita (POL)
To: Rivera Morgan, Awilda (POL)
Subject: FW: FJAGHEOP16 5TH DIVISION
Date: Wednesday, November 29, 2017 11:24:17 AM
Attachments: POL - FJAGHEOP16.doc

Can you review the attachment A.

Thanks

From: Sojka, Robert (POL)
Sent: Wednesday, November 29, 2017 11:04 AM
To: Taylor, Rita (POL)
Subject: RE: FJAGHEOP16 5TH DIVISION

Can you give this a quick look to be sure it is acceptable?

-Bob

From: Taylor, Rita (POL)
Sent: Tuesday, November 28, 2017 4:15 PM
To: Sojka, Robert (POL)
Subject: FJAGHEOP16 5TH DIVISION
Importance: High

Hi , could you please complete the attachment A initial each page of the ISA , and complete the Project Manager Responsibilities form.

Please let me know if you have any questions.

Thanks

Rita
Rita Taylor
Grant Administrator/Acting Payroll Director
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2151
Rita.Taylor@State.Ma.US

From: Maloney, Colleen (OGR)
Sent: Tuesday, November 28, 2017 2:33 PM

To: Taylor, Rita (POL)
Subject:
Importance: High

Hi Rita,

I want to make sure I get these to the right person, are you going to be handling the grant info for MSPs new 5th division? If so attached are the ISA documents, could you please get them signed and sent back?

Thanks!
Colleen

Colleen Maloney
Justice and Prevention
Executive Office of Public Safety and Security/OGR
Ten Park Plaza, Suite 3720
Boston, MA 02116
617-725-3316

From: Taylor, Rita (POL)
To: Rivera Morgan, Awilda (POL)
Subject: FW: FJAGHEOP16 5TH DIVISION
Date: Wednesday, November 29, 2017 11:24:00 AM
Attachments: POL - FJAGHEOP16.doc

Can you review the attachment A.

Thanks

From: Sojka, Robert (POL)
Sent: Wednesday, November 29, 2017 11:04 AM
To: Taylor, Rita (POL)
Subject: RE: FJAGHEOP16 5TH DIVISION

Can you give this a quick look to be sure it is acceptable?

-Bob

From: Taylor, Rita (POL)
Sent: Tuesday, November 28, 2017 4:15 PM
To: Sojka, Robert (POL)
Subject: FJAGHEOP16 5TH DIVISION
Importance: High

Hi , could you please complete the attachment A initial each page of the ISA , and complete the Project Manager Responsibilities form.

Please let me know if you have any questions.

Thanks

Rita
Rita Taylor
Grant Administrator/Acting Payroll Director
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2151
Rita.Taylor@State.Ma.US

From: Maloney, Colleen (OGR)
Sent: Tuesday, November 28, 2017 2:33 PM

To: Taylor, Rita (POL)
Subject:
Importance: High

Hi Rita,

I want to make sure I get these to the right person, are you going to be handling the grant info for MSPs new 5th division? If so attached are the ISA documents, could you please get them signed and sent back?

Thanks!
Colleen

Colleen Maloney
Justice and Prevention
Executive Office of Public Safety and Security/OGR
Ten Park Plaza, Suite 3720
Boston, MA 02116
617-725-3316

From: Taylor, Rita (POL)
To: Sojka, Robert (POL)
Subject: FW: FJAGHEOP16 5TH DIVISION
Date: Wednesday, November 29, 2017 12:57:01 PM
Attachments: ISA FJAGHEOP16 5TH DIVISION ALPR purchases - Attachment A.doc

Hi we made a few changes in the equipment section. We prefer to not list it all out in case a particular model/brand is not available. Please review and if you are agreement please initial all pages of the terms and conditions and return to me.

Thanks

Rita

From: Taylor, Rita (POL)
Sent: Wednesday, November 29, 2017 11:24 AM
To: Rivera Morgan, Awilda (POL)
Subject: FW: FJAGHEOP16 5TH DIVISION

Can you review the attachment A.

Thanks

From: Sojka, Robert (POL)
Sent: Wednesday, November 29, 2017 11:04 AM
To: Taylor, Rita (POL)
Subject: RE: FJAGHEOP16 5TH DIVISION

Can you give this a quick look to be sure it is acceptable?

-Bob

From: Taylor, Rita (POL)
Sent: Tuesday, November 28, 2017 4:15 PM
To: Sojka, Robert (POL)
Subject: FJAGHEOP16 5TH DIVISION
Importance: High

Hi , could you please complete the attachment A initial each page of the ISA , and complete the Project Manager Responsibilities form.

Please let me know if you have any questions.

Thanks

Rita
Rita Taylor

Grant Administrator/Acting Payroll Director
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
508-820-2151
Rita.Taylor@State.Ma.US

From: Maloney, Colleen (OGR)
Sent: Tuesday, November 28, 2017 2:33 PM
To: Taylor, Rita (POL)
Subject:
Importance: High

Hi Rita,

I want to make sure I get these to the right person, are you going to be handling the grant info for MSPs new 5th division? If so attached are the ISA documents, could you please get them signed and sent back?

Thanks!
Colleen

Colleen Maloney
Justice and Prevention
Executive Office of Public Safety and Security/OGR
Ten Park Plaza, Suite 3720
Boston, MA 02116
617-725-3316

From: Fenton, Eileen (DOT)
To: Amodeo, Edward (POL); Quinn, Dermot (POL); Halpin, Michael (POL); Hanson, Terry (POL)
Subject: FW: MOU Re: ALPR on MassDOT Property
Date: Tuesday, April 4, 2017 4:21:04 PM
Attachments: ALPR Agreement 24925.doc

Good Afternoon,
Attached for your review and comment is a draft of the MOU between MassDOT and the State Police for installation of ALPR equipment on MassDOT property. As discussed, the agreement is not site specific. In the event you are interested in a specific location, the agreement provides that you will submit the plans to MassDOT for review and approval, as appropriate.

Once I receive your comments, I will send along to Tom Tinlin for review.

Please let me know if you have any questions.

Thank you.
Eileen

Eileen M. Fenton
Senior Counsel
Massachusetts Department of Transportation
Ten Park Plaza, Suite 3510
Boston, Massachusetts 02116
T: 857-368-8764
Eileen.Fenton@state.ma.us

From: Halpin, Michael (POL)
To: Hiitt, Katelyn (POL)
Cc: Farrell, Sean (POL)
Subject: FW: MOU Re: ALPR on MassDOT Property
Date: Tuesday, April 4, 2017 5:20:02 PM
Attachments: ALPR Agreement 24925.doc

Sean: Please review and see me to discuss. Thanks.

From: Fenton, Eileen (DOT) [mailto:eileen.fenton@dot.state.ma.us]
Sent: Tuesday, April 04, 2017 4:18 PM
To: Amodeo, Edward (POL); Quinn, Dermot (POL); Halpin, Michael (POL); Hanson, Terry (POL)
Subject: FW: MOU Re: ALPR on MassDOT Property

Good Afternoon,
Attached for your review and comment is a draft of the MOU between MassDOT and the State Police for installation of ALPR equipment on MassDOT property. As discussed, the agreement is not site specific. In the event you are interested in a specific location, the agreement provides that you will submit the plans to MassDOT for review and approval, as appropriate.

Once I receive your comments, I will send along to Tom Tinlin for review.

Please let me know if you have any questions.

Thank you.
Eileen

Eileen M. Fenton
Senior Counsel
Massachusetts Department of Transportation
Ten Park Plaza, Suite 3510
Boston, Massachusetts 02116
T: 857-368-8764
Eileen.Fenton@state.ma.us

From: Pellegrino, Paul (POL)
To: Farley, Michael (POL); Grasso, Jimi (POL)
Subject: FW: Nlets Training PowerPoint Presentation
Date: Monday, November 6, 2017 9:02:00 AM
Attachments: Nlets Training for Massachusetts - 11.01.17.pptx
image002.png
image003.png

DLT/LT
The attached Power Point is from a recent Nlets training.
I found the PP, to be very informative and might be a good refresh of the capabilities of Nlets for the members of VFAS.

Paul J. Pellegrino, Esq.
Special Projects Manager
Massachusetts State Police
Violent Fugitive Apprehension Section
Office (508) 820-2384

From: Dunne, Michaela (CHS)
Sent: Friday, November 03, 2017 11:41 AM
To: Dunne, Michaela (CHS)
Cc: Hutchinson, Daniel (CHS)
Subject: Nlets Training PowerPoint Presentation

Good Morning,

Thank you to all who were able attend the Nlets training on November 1. We hope that you and/or your staff found the information to be helpful.

I have attached the PowerPoint presentation to this email. Please forward to your staff that attended the training, or anyone who was unable to attend but may find the information useful. This has also been uploaded to the DCJIS Extranet (only accessible via computers with access to CJIS) under the "Documents and Manuals" tab: http://170.154.225.103/default.aspx.

As always, if you have any questions about the Nlets transactions covered at the training, or any other CJIS related questions, do not hesitate to contact the CJIS Support Services Unit at 617.660.4710 or via email at cjis.support@state.ma.us.

Thank you,

Michaela Dunne | Manager of Law Enforcement & Justice Services
Massachusetts Department of Criminal Justice Information Services
200 Arlington Street, Suite 2200
Chelsea, MA 02150
p. 617.660.4682 | f. 617.884.4601
michaela.dunne@state.ma.us | mass.gov/cjis

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: Ardizzoni, Alyssa (CHS)
Sent: Thursday, October 26, 2017 11:11 AM
ToCc: Hutchinson, Daniel (CHS); Dunne, Michaela (CHS)
Subject: Reminder: Nlets Training Announcement - November 1, 2017

Good Morning,

The Department of Criminal Justice Information Services (DCJIS) is pleased to host Ms. Teri Fournier-Harsin, Nlets Training Manager, for a comprehensive Nlets training on November 1. This training will cover topics including the importance of nationwide information sharing as well as overviews of many of the specific Nlets queries available for law enforcement officers and personnel through the Massachusetts Criminal Justice Information System (CJIS).

This training is open to all CJIS Representatives and any other officer or employee who currently utilizes the Nlets queries through CJIS. There is no cost to attend this training.

DATE: Wednesday, November 1
TIME: 9:00am to 2:00pm
LOCATION: Kowloon Restaurant
948 Broadway
Saugus, MA 01906

Pre-registration is required on the DCJIS Extranet: http://170.154.225.103/trainingannouncements1/default.aspx. You need to be using a computer that has access to the CJIS System to access this link.

For additional information, please call the CJIS Support Services Unit at 617.660.4710.

Sincerely,

Alyssa Ardizzoni | CJIS Representative
Massachusetts Department of Criminal Justice Information Services
CJIS Support Services
200 Arlington Street, Suite 2200
Chelsea, MA 02150
t: 617.660.4711| f: 617.884.4601
Alyssa.ardizzoni@state.ma.us| http://www.mass.gov/cjis

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: Underwood, Pamela (POL)
To: Leblanc, Jeffrey (POL); Blomgren, Robert (POL); Butler, Michael (POL); Roy, Robert (POL); Kumiega, Annette (POL); Sawicki, Scott (POL); McGrail, Francis (POL); Silbor, David (POL); Canale, Robert (POL); TRUE, Charles (POL); Medina, William (POL); Marsh, Jeffrey (POL); Monteiro, Pedro (POL); Gamelli, Anthony (POL); Uliana, Christopher (POL); Sao, Alexander (POL); Hall, Aimee (POL); Bova, Anthony (POL); Zanni, Gregory (POL)
Subject: Fw: Nlets Training PowerPoint Presentation
Date: Friday, November 3, 2017 1:20:39 PM
Attachments: Nlets Training for Massachusetts - 11.01.17.pptx

---

Hello all,

I went to CJIS training this past week for NLETS, NLETS is a private group that facilitates information exchange for LE through their interchange. They are a great investigative resource housing a lot of different queries that may prove useful to you. They provide an interface with Interpol, Canada, certain participating states for Sex Offender Registry, hunting license data, human intelligence, boat files, gun files, License Plate Readers (I.e see if a wanted plate has been read anywhere else) and tracing of the id tags at a taser deployment (LE ones exempt, those have been redacted and you must go through the company), etc. There are a world of resources available to you. Please take a few minutes to read through the slides it is worth the effort.

They also wanted to remind people that there is also EPIC (El Paso Intelligence Center) which can provide access to Mexican driver's license photos, other foreign access etc. They have representatives there from different entities that can assist you.

It really was interesting and worth the effort to peruse these slides.

Thanks,
Pam

Trooper Pamela J. Underwood #1414
S&P Belchertown C-7
485 Ware Road
Belchertown, Ma. 01007
413-323-7561
Fax 413-323-6499

From: Dunne, Michaela (CHS)
Sent: Friday, November 3, 2017 11:40 AM
To: Dunne, Michaela (CHS)
Cc: Hutchinson, Daniel (CHS)
Subject: Nlets Training PowerPoint Presentation

Good Morning,

Thank you to all who were able attend the Nlets training on November 1. We hope that you and/or your staff found the information to be helpful.

I have attached the PowerPoint presentation to this email. Please forward to your staff that

attended the training, or anyone who was unable to attend but may find the information useful. This has also been uploaded to the DCJIS Extranet (only accessible via computers with access to CJIS) under the "Documents and Manuals" tab: http://170.154.225.103/default.aspx.

As always, if you have any questions about the Nlets transactions covered at the training, or any other CJIS related questions, do not hesitate to contact the CJIS Support Services Unit at 617.660.4710 or via email at cjis.support@state.ma.us.

Thank you,

Michaela Dunne | Manager of Law Enforcement & Justice Services
Massachusetts Department of Criminal Justice Information Services
200 Arlington Street, Suite 2200
Chelsea, MA 02150
p. 617.660.4682 | f. 617.884.4601
michaela.dunne@state.ma.us | mass.gov/cjis

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: Ardizzoni, Alyssa (CHS)
Sent: Thursday, October 26, 2017 11:11 AM
ToCc: Hutchinson, Daniel (CHS); Dunne, Michaela (CHS)
Subject: Reminder: Nlets Training Announcement - November 1, 2017

Good Morning,

The Department of Criminal Justice Information Services (DCJIS) is pleased to host Ms. Teri Fournier-Harsin, Nlets Training Manager, for a comprehensive Nlets training on November 1. This training will cover topics including the importance of nationwide information sharing as well as overviews of many of the specific Nlets queries available for law enforcement officers and personnel through the Massachusetts Criminal Justice Information System (CJIS).

This training is open to all CJIS Representatives and any other officer or employee who currently utilizes the Nlets queries through CJIS. There is no cost to attend this training.

DATE: Wednesday, November 1
TIME: 9:00am to 2:00pm
LOCATION: Kowloon Restaurant
948 Broadway
Saugus, MA 01906

Pre-registration is required on the DCJIS Extranet: http://170.154.225.103/trainingannouncements1/default.aspx. You need to be using a computer that has access to the CJIS System to access this link.

For additional information, please call the CJIS Support Services Unit at 617.660.4710.

Sincerely,

Alyssa Ardizzoni | CJIS Representative
Massachusetts Department of Criminal Justice Information Services
CJIS Support Services
200 Arlington Street, Suite 2200
Chelsea, MA 02150
t: 617.660.4711| f: 617.884.4601
Alyssa.ardizzoni@state.ma.us| http://www.mass.gov/cjis

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: Tapis, Stephen C (POL)
To: Jordan Plachecki [KHP] (Jordan.Plachecki@KS.GOV)
Subject: FW: SPPPOS Request for LPR regulations
Date: Wednesday, March 22, 2017 10:42:00 AM
Attachments: LPR Bill.pdf

Good morning-

Please find attached the Statute regarding LPRs.

Respectfully-

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

From: spppo@theiacp.simplelists.com [mailto:spppo@theiacp.simplelists.com] **On Behalf Of** Jordan Plachecki [KHP]
Sent: Friday, March 17, 2017 2:45 PM
To: 'spppo@theiacp.simplelists.com'
Subject: SPPPOS Request for LPR regulations

Fellow Planners,
The Kansas Highway Patrol is looking for states that are using mobile license plate readers (LPRs) that don't have any statues in place regulating their use.

1) Does your states use LPRs without statutory regulation?

2) Does your state use LPRs and have a statute regulating their use? If so, please send us a copy of the statute.

Any information you can provide will be greatly appreciated. If you provided information to our other related SPPPOS request THANK YOU! Please send responses to jordan.plachecki@ks.gov.

Technical Trooper Jordan Plachecki
Public & Governmental Affairs
Kansas Highway Patrol
122 SW 7th Street
Topeka, KS 66603
Office (785)296-8826
Cell (785)250-8296
Fax (785)296-5956
jordan.plachecki@ks.gov

To unsubscribe from this list please go to
http://www.simplelists.com/confirm.php?u=tmZIXsOGZ5qy9aqjgxyzuOjDcJegobkt

From:	Eldridge, Kimberly (POL)
To:	Handfield, Kenneth (POL); McKinnon, Stephanie (POL); Marshall, Harold (POL); McCann, Joseph M (POL); Demers, Joanne (POL); DeCosta, David T (POL); Gordon, Victoria (POL); Jones, Christine (POL); Chaves, Daniel (POL); Swiers, Brian (POL); Brown, Heather (POL); Fredholm, Shana (POL); Ronayne, Adam (POL); McKinnon, Stephanie (POL); Eldridge, Kimberly (POL)
Subject:	Fw: User manual
Date:	Sunday, February 12, 2017 7:51:59 AM
Attachments:	BOSS_3.2x_User_Manual_final.pdf image001.png

From: Griffin, Daniel (POL)
Sent: Friday, February 10, 2017 9:42 AM
To: Eldridge, Kimberly (POL)
Subject: User manual

☺ user manual for plate reader in case anybody needs it!

Lieutenant Daniel J. Griffin 1129
Massachusetts State Police
Traffic Programs Section
General Headquarters
470 Worcester Rd
Framingham, Ma. 01702
508-988-7404
daniel.griffin@massmail.state.ma.us

From: Donna Lindquist
To: Donna Lindquist
Subject: Get Ready! NFCA 2017 Training Event - "Roadmap to Our Sponsors"
Date: Wednesday, November 1, 2017 7:27:14 PM
Attachments: image001.png
image002.png
2017 NFCA Sponsor Roadmap Booklet.pdf

Greetings, **2017 National Fusion Center Association (NFCA) Training Event** Attendees!

We look forward to welcoming you to the exciting annual NFCA training and networking opportunity in just a few days—**November 7–9**—at the **Hilton Alexandria Mark Center hotel**.

Thank you for your commitment to the National Network of Fusion Centers and to safeguarding our neighborhoods and securing our Nation through your dedication:

- As critical members in the fusion center, intelligence, and analyst communities.
- As force-multiplying partners and stakeholders.
- As private sector innovators.

To help gear up for productive and enjoyable networking breaks, we are pleased to provide the **attached "*Roadmap to Our Sponsors*,"** showcasing products and services from our premier patrons. Please take a few minutes to preview the impressive range of offerings and plan your tour of the exhibition lobbies for further exploration and face-to-face conversations. **Your engagement with all of our industry partners is very important:** we are only able to hold these NFCA Training Events because of their generous support. Thank you for stopping by for a few minutes at each booth and saying hello!

Best regards,

Donna Jean Lindquist
Phone: 850.766.9806
E-mail: dlindquist@iir.com

Learn how the National Fusion Center Association is helping to protect America at https://nfcausa.org/.

Thank You to our Sponsors

Platinum

esri
THE SCIENCE OF WHERE

Award

IBM

Gold

CARFAX · MSAB · VERITONE government · FirstNet

Silver

A·C·I·S·S · Hiperwall · VIGILANT SOLUTIONS · Vision Logic · ANOMALI · WHOOSTER.COM · GeoTime · THOMSON REUTERS · verecity · Adobe · LUMEN · TRAPWIRE · neustar · Haystax

Specialty Sponsors

A·C·I·S·S · NS2 · collette guided by travel · MOTOROLA · FirstNet

Exhibitors

PEN·LINK · MOTOROLA · CRIMENTEL · SAS · welund north america · MEDIA SONAR · Mutualink · Global Intel Tip Management Software · report it · Forensic Logic · vintra · SINTELIX · EagleEye · DHS Office for Bombing Prevention · Harmari by LTAS

From: PoliceOne Product Alert
To: Lyver, Michael (POL)
Subject: Headed to IACP 2017? Don"t miss these booths.
Date: Tuesday, October 10, 2017 11:11:10 AM

October 10, 2017 | View as webpage

Download the Mobile App

Spillman Flex: Software that Works the Way You Do

What kind of system would your agency build? Spillman Flex provides a flexible, off-the-shelf software solution to support each public safety agency's specific needs and pain points.

Visit us at booth #3037

Preview L3 Mobile Vision's Latest Products at IACP

Get a free T-shirt and a chance to win a set of four Disney park passes when you demo our new Cloud-Based Evidence Management System in our booth at IACP! You don't want to miss this.

Visit us at booth #2549

Still Wasting Your Precious Time and Money?

Dummies Unlimited's proven training products allow your officers to realistically practice de-escalation techniques. Save your agency time and money and reduce liability!

Visit us at booth #3601

Introducing the FATS® 100P: Portable Virtual Training

The lightweight FATS 100P platform features video authoring, judgmental and marksmanship training, and automatic coaching for up to 6 weapons — all in an easily transportable laptop.

Visit us at booth #1909

Don't Miss the Action in IACP Booth 1937!

Experience our new ALPR technologies, engineered to assist with a variety of functions from real-time interdiction to traffic data collection and tolling. Save your agency time and money!

Visit us at booth #1937

Protect Everyone: Demo Our Fully Adjustable Riot Suit

The new Tac Commander™ Riot and Crowd Control Gear is fully adjustable to fit virtually everyone. Join us at IACP for beverages, giveaways, training, and more!

Visit us at booth #1725

Quantifit® The Gold Standard of Respirator Fit Testing

Within ten seconds of testing, the Quantifit determines if the respirator user has a basic fit. No other quantitative fit test instrument comes close!

Visit us at booth #3808

FLIR Thermal Imaging at IACP

Thermal optics are more affordable than ever. Stop by Booth #4009 and see FLIR's suite of high-performance tactical imagers for yourself.

Visit us at booth #4009

Axon is IN for IACP. Are you?

We'll be showing our latest (and future) technologies, including new AI-powered apps and other products, and unveiling a new campaign.

Visit us at booth #2825

Making It Safer: Collaborating To Advance Officer Safety and Wellness

Award Categories: General Officer Safety, Officers Traffic Safety, Officer Wellness, and Comprehensive Safety. Submit your program today!

Visit us at booth #2403

Making It Safer: A Report on Law Enforcement Fatalities

Did you know that 'Domestic Dispute' calls account for 29% of fatal calls for service? Join as at IACP to see how you can improve your odds!

Visit us at booth #2403

Want Real-Time Access to Over $8 billion in LE Grants?

Powered by PoliceOne and PoliceGrantsHelp, Police GrantFinder is the ultimate law enforcement grant search tool made for you.

Visit us at booth #1448

This message was sent to michael.lyver@pol.state.ma.us from:

PoliceOne Product Alert | ProductAlerts@policeone.com | Praetorian Digital | 200 Green St Suite 200 | San Francisco, California 94111

Unsubscribe

From: PoliceOne Product Alert
To: Smith, George (POL)
Subject: Headed to IACP 2017? Don"t miss these booths.
Date: Tuesday, October 10, 2017 11:10:27 AM

October 10, 2017 | View as webpage

Download the Mobile App

Spillman Flex: Software that Works the Way You Do

What kind of system would your agency build? Spillman Flex provides a flexible, off-the-shelf software solution to support each public safety agency's specific needs and pain points.

Visit us at booth #3037

Preview L3 Mobile Vision's Latest Products at IACP

Get a free T-shirt and a chance to win a set of four Disney park passes when you demo our new Cloud-Based Evidence Management System in our booth at IACP! You don't want to miss this.

Visit us at booth #2549

Still Wasting Your Precious Time and Money?

Dummies Unlimited's proven training products allow your officers to realistically practice de-escalation techniques. Save your agency time and money and reduce liability!

Visit us at booth #3601

Introducing the FATS® 100P: Portable Virtual Training

The lightweight FATS 100P platform features video authoring, judgmental and marksmanship training, and automatic coaching for up to 6 weapons — all in an easily transportable laptop.

Visit us at booth #1909

Don't Miss the Action in IACP Booth 1937!

Experience our new ALPR technologies, engineered to assist with a variety of functions from real-time interdiction to traffic data collection and tolling. Save your agency time and money!

Visit us at booth #1937

Protect Everyone: Demo Our Fully Adjustable Riot Suit

The new Tac Commander™ Riot and Crowd Control Gear is fully adjustable to fit virtually everyone. Join us at IACP for beverages, giveaways, training, and more!

Visit us at booth #1725

Quantifit® The Gold Standard of Respirator Fit Testing

Within ten seconds of testing, the Quantifit determines if the respirator user has a basic fit. No other quantitative fit test instrument comes close!

Visit us at booth #3808

FLIR Thermal Imaging at IACP

Thermal optics are more affordable than ever. Stop by Booth #4009 and see FLIR's suite of high-performance tactical imagers for yourself.

Visit us at booth #4009

Axon is IN for IACP. Are you?

We'll be showing our latest (and future) technologies, including new AI-powered apps and other products, and unveiling a new campaign.

Visit us at booth #2825

Making It Safer: Collaborating To Advance Officer Safety and Wellness

Award Categories: General Officer Safety, Officers Traffic Safety, Officer Wellness, and Comprehensive Safety. Submit your program today!

Visit us at booth #2403

Making It Safer: A Report on Law Enforcement Fatalities

Did you know that 'Domestic Dispute' calls account for 29% of fatal calls for service? Join as at IACP to see how you can improve your odds!

Visit us at booth #2403

Want Real-Time Access to Over $8 billion in LE Grants?

Powered by PoliceOne and PoliceGrantsHelp, Police GrantFinder is the ultimate law enforcement grant search tool made for you.

Visit us at booth #1448

This message was sent to george.smith@pol.state.ma.us from:

PoliceOne Product Alert | ProductAlerts@policeone.com | Praetorian Digital | 200 Green St Suite 200 | San Francisco, California 94111

Unsubscribe

From: PoliceOne Product Alert
To: Silva, Patrick (POL)
Subject: Headed to IACP 2017? Don"t miss these booths.
Date: Tuesday, October 10, 2017 11:08:59 AM

October 10, 2017 | View as webpage

Download the Mobile App

Spillman Flex: Software that Works the Way You Do

What kind of system would your agency build? Spillman Flex provides a flexible, off-the-shelf software solution to support each public safety agency's specific needs and pain points.

Visit us at booth #3037

Preview L3 Mobile Vision's Latest Products at IACP

Get a free T-shirt and a chance to win a set of four Disney park passes when you demo our new Cloud-Based Evidence Management System in our booth at IACP! You don't want to miss this.

Visit us at booth #2549

Still Wasting Your Precious Time and Money?

Dummies Unlimited's proven training products allow your officers to realistically practice de-escalation techniques. Save your agency time and money and reduce liability!

Visit us at booth #3601

Introducing the FATS® 100P: Portable Virtual Training

The lightweight FATS 100P platform features video authoring, judgmental and marksmanship training, and automatic coaching for up to 6 weapons — all in an easily transportable laptop.

Visit us at booth #1909

Don't Miss the Action in IACP Booth 1937!

Experience our new ALPR technologies, engineered to assist with a variety of functions from real-time interdiction to traffic data collection and tolling. Save your agency time and money!

Visit us at booth #1937

Protect Everyone: Demo Our Fully Adjustable Riot Suit

The new Tac Commander™ Riot and Crowd Control Gear is fully adjustable to fit virtually everyone. Join us at IACP for beverages, giveaways, training, and more!

Visit us at booth #1725

Quantifit® The Gold Standard of Respirator Fit Testing

Within ten seconds of testing, the Quantifit determines if the respirator user has a basic fit. No other quantitative fit test instrument comes close!

Visit us at booth #3808

FLIR Thermal Imaging at IACP

Thermal optics are more affordable than ever. Stop by Booth #4009 and see FLIR's suite of high-performance tactical imagers for yourself.

Visit us at booth #4009

Axon is IN for IACP. Are you?

We'll be showing our latest (and future) technologies, including new AI-powered apps and other products, and unveiling a new campaign.

Visit us at booth #2825

Making It Safer: Collaborating To Advance Officer Safety and Wellness

Award Categories: General Officer Safety, Officers Traffic Safety, Officer Wellness, and Comprehensive Safety. Submit your program today!

Visit us at booth #2403

Making It Safer: A Report on Law Enforcement Fatalities

Did you know that 'Domestic Dispute' calls account for 29% of fatal calls for service? Join as at IACP to see how you can improve your odds!

Visit us at booth #2403

Want Real-Time Access to Over $8 billion in LE Grants?

Powered by PoliceOne and PoliceGrantsHelp, Police GrantFinder is the ultimate law enforcement grant search tool made for you.

Visit us at booth #1448

This message was sent to patrick.silva@pol.state.ma.us from:

PoliceOne Product Alert | ProductAlerts@policeone.com | Praetorian Digital | 200 Green St Suite 200 | San Francisco, California 94111

Unsubscribe

From: PoliceOne Product Alert
To: Conneely, Paul (POL)
Subject: Headed to IACP 2017? Don"t miss these booths.
Date: Tuesday, October 10, 2017 11:08:56 AM

October 10, 2017 | View as webpage

Download the Mobile App

Spillman Flex: Software that Works the Way You Do

What kind of system would your agency build? Spillman Flex provides a flexible, off-the-shelf software solution to support each public safety agency's specific needs and pain points.

Visit us at booth #3037

Preview L3 Mobile Vision's Latest Products at IACP

Get a free T-shirt and a chance to win a set of four Disney park passes when you demo our new Cloud-Based Evidence Management System in our booth at IACP! You don't want to miss this.

Visit us at booth #2549

Still Wasting Your Precious Time and Money?

Dummies Unlimited's proven training products allow your officers to realistically practice de-escalation techniques. Save your agency time and money and reduce liability!

Visit us at booth #3601

Introducing the FATS® 100P: Portable Virtual Training

The lightweight FATS 100P platform features video authoring, judgmental and marksmanship training, and automatic coaching for up to 6 weapons — all in an easily transportable laptop.

Visit us at booth #1909

Don't Miss the Action in IACP Booth 1937!

Experience our new ALPR technologies, engineered to assist with a variety of functions from real-time interdiction to traffic data collection and tolling. Save your agency time and money!

Visit us at booth #1937

Protect Everyone: Demo Our Fully Adjustable Riot Suit

The new Tac Commander™ Riot and Crowd Control Gear is fully adjustable to fit virtually everyone. Join us at IACP for beverages, giveaways, training, and more!

Visit us at booth #1725

Quantifit® The Gold Standard of Respirator Fit Testing

Within ten seconds of testing, the Quantifit determines if the respirator user has a basic fit. No other quantitative fit test instrument comes close!

Visit us at booth #3808

FLIR Thermal Imaging at IACP

Thermal optics are more affordable than ever. Stop by Booth #4009 and see FLIR's suite of high-performance tactical imagers for yourself.

Visit us at booth #4009

Axon is IN for IACP. Are you?

We'll be showing our latest (and future) technologies, including new AI-powered apps and other products, and unveiling a new campaign.

Visit us at booth #2825

Making It Safer: Collaborating To Advance Officer Safety and Wellness

Award Categories: General Officer Safety, Officers Traffic Safety, Officer Wellness, and Comprehensive Safety. Submit your program today!

Visit us at booth #2403

Making It Safer: A Report on Law Enforcement Fatalities

Did you know that 'Domestic Dispute' calls account for 29% of fatal calls for service? Join as at IACP to see how you can improve your odds!

Visit us at booth #2403

Want Real-Time Access to Over $8 billion in LE Grants?

Powered by PoliceOne and PoliceGrantsHelp, Police GrantFinder is the ultimate law enforcement grant search tool made for you.

Visit us at booth #1448

This message was sent to paul.conneely@massmail.state.ma.us from:

PoliceOne Product Alert | ProductAlerts@policeone.com | Praetorian Digital | 200 Green St Suite 200 | San Francisco, California 94111

Unsubscribe

From: PoliceOne Product Alert
To: Davis, Matthew (POL)
Subject: Headed to IACP 2017? Don"t miss these booths.
Date: Tuesday, October 10, 2017 11:08:42 AM

October 10, 2017 | View as webpage

Download the Mobile App

Spillman Flex: Software that Works the Way You Do

What kind of system would your agency build? Spillman Flex provides a flexible, off-the-shelf software solution to support each public safety agency's specific needs and pain points.

Visit us at booth #3037

Preview L3 Mobile Vision's Latest Products at IACP

Get a free T-shirt and a chance to win a set of four Disney park passes when you demo our new Cloud-Based Evidence Management System in our booth at IACP! You don't want to miss this.

Visit us at booth #2549

Still Wasting Your Precious Time and Money?

Dummies Unlimited's proven training products allow your officers to realistically practice de-escalation techniques. Save your agency time and money and reduce liability!

Visit us at booth #3601

Introducing the FATS® 100P: Portable Virtual Training

The lightweight FATS 100P platform features video authoring, judgmental and marksmanship training, and automatic coaching for up to 6 weapons — all in an easily transportable laptop.

Visit us at booth #1909

Don't Miss the Action in IACP Booth 1937!

Experience our new ALPR technologies, engineered to assist with a variety of functions from real-time interdiction to traffic data collection and tolling. Save your agency time and money!

Visit us at booth #1937

Protect Everyone: Demo Our Fully Adjustable Riot Suit

The new Tac Commander™ Riot and Crowd Control Gear is fully adjustable to fit virtually everyone. Join us at IACP for beverages, giveaways, training, and more!

Visit us at booth #1725

Quantifit® The Gold Standard of Respirator Fit Testing

Within ten seconds of testing, the Quantifit determines if the respirator user has a basic fit. No other quantitative fit test instrument comes close!

Visit us at booth #3808

FLIR Thermal Imaging at IACP

Thermal optics are more affordable than ever. Stop by Booth #4009 and see FLIR's suite of high-performance tactical imagers for yourself.

Visit us at booth #4009

Axon is IN for IACP. Are you?

We'll be showing our latest (and future) technologies, including new AI-powered apps and other products, and unveiling a new campaign.

Visit us at booth #2825

Making It Safer: Collaborating To Advance Officer Safety and Wellness

Award Categories: General Officer Safety, Officers Traffic Safety, Officer Wellness, and Comprehensive Safety. Submit your program today!

Visit us at booth #2403

Making It Safer: A Report on Law Enforcement Fatalities

Did you know that 'Domestic Dispute' calls account for 29% of fatal calls for service? Join as at IACP to see how you can improve your odds!

Visit us at booth #2403

Want Real-Time Access to Over $8 billion in LE Grants?

Powered by PoliceOne and PoliceGrantsHelp, Police GrantFinder is the ultimate law enforcement grant search tool made for you.

Visit us at booth #1448

This message was sent to matthew.davis@pol.state.ma.us from:

PoliceOne Product Alert | ProductAlerts@policeone.com | Praetorian Digital | 200 Green St Suite 200 | San Francisco, California 94111

Unsubscribe

From: PoliceOne Product Alert
To: Grasso, Jimi (POL)
Subject: Headed to IACP 2017? Don"t miss these booths.
Date: Tuesday, October 10, 2017 11:07:58 AM

October 10, 2017 | View as webpage

Download the Mobile App

Spillman Flex: Software that Works the Way You Do

What kind of system would your agency build? Spillman Flex provides a flexible, off-the-shelf software solution to support each public safety agency's specific needs and pain points.

Visit us at booth #3037

Preview L3 Mobile Vision's Latest Products at IACP

Get a free T-shirt and a chance to win a set of four Disney park passes when you demo our new Cloud-Based Evidence Management System in our booth at IACP! You don't want to miss this.

Visit us at booth #2549

Still Wasting Your Precious Time and Money?

Dummies Unlimited's proven training products allow your officers to realistically practice de-escalation techniques. Save your agency time and money and reduce liability!

Visit us at booth #3601

Introducing the FATS® 100P: Portable Virtual Training

The lightweight FATS 100P platform features video authoring, judgmental and marksmanship training, and automatic coaching for up to 6 weapons — all in an easily transportable laptop.

Visit us at booth #1909

Don't Miss the Action in IACP Booth 1937!

Experience our new ALPR technologies, engineered to assist with a variety of functions from real-time interdiction to traffic data collection and tolling. Save your agency time and money!

Visit us at booth #1937

Protect Everyone: Demo Our Fully Adjustable Riot Suit

The new Tac Commander™ Riot and Crowd Control Gear is fully adjustable to fit virtually everyone. Join us at IACP for beverages, giveaways, training, and more!

Visit us at booth #1725

Quantifit® The Gold Standard of Respirator Fit Testing

Within ten seconds of testing, the Quantifit determines if the respirator user has a basic fit. No other quantitative fit test instrument comes close!

Visit us at booth #3808

FLIR Thermal Imaging at IACP

Thermal optics are more affordable than ever. Stop by Booth #4009 and see FLIR's suite of high-performance tactical imagers for yourself.

Visit us at booth #4009

Axon is IN for IACP. Are you?

We'll be showing our latest (and future) technologies, including new AI-powered apps and other products, and unveiling a new campaign.

Visit us at booth #2825

Making It Safer: Collaborating To Advance Officer Safety and Wellness

Award Categories: General Officer Safety, Officers Traffic Safety, Officer Wellness, and Comprehensive Safety. Submit your program today!

Visit us at booth #2403

Making It Safer: A Report on Law Enforcement Fatalities

Did you know that 'Domestic Dispute' calls account for 29% of fatal calls for service? Join as at IACP to see how you can improve your odds!

Visit us at booth #2403

Want Real-Time Access to Over $8 billion in LE Grants?

Powered by PoliceOne and PoliceGrantsHelp, Police GrantFinder is the ultimate law enforcement grant search tool made for you.

Visit us at booth #1448

This message was sent to jimi.grasso@pol.state.ma.us from:

PoliceOne Product Alert | ProductAlerts@policeone.com | Praetorian Digital | 200 Green St Suite 200 | San Francisco, California 94111

Unsubscribe

From: PoliceOne Product Alert
To: Somerville, Arthur (POL)
Subject: Headed to IACP 2017? Don"t miss these booths.
Date: Tuesday, October 10, 2017 11:07:38 AM

October 10, 2017 | View as webpage

Download the Mobile App

Spillman Flex: Software that Works the Way You Do

What kind of system would your agency build? Spillman Flex provides a flexible, off-the-shelf software solution to support each public safety agency's specific needs and pain points.

Visit us at booth #3037

Preview L3 Mobile Vision's Latest Products at IACP

Get a free T-shirt and a chance to win a set of four Disney park passes when you demo our new Cloud-Based Evidence Management System in our booth at IACP! You don't want to miss this.

Visit us at booth #2549

Still Wasting Your Precious Time and Money?

Dummies Unlimited's proven training products allow your officers to realistically practice de-escalation techniques. Save your agency time and money and reduce liability!

Visit us at booth #3601

Introducing the FATS® 100P: Portable Virtual Training

The lightweight FATS 100P platform features video authoring, judgmental and marksmanship training, and automatic coaching for up to 6 weapons — all in an easily transportable laptop.

Visit us at booth #1909

Don't Miss the Action in IACP Booth 1937!

Experience our new ALPR technologies, engineered to assist with a variety of functions from real-time interdiction to traffic data collection and tolling. Save your agency time and money!

Visit us at booth #1937

Protect Everyone: Demo Our Fully Adjustable Riot Suit

The new Tac Commander™ Riot and Crowd Control Gear is fully adjustable to fit virtually everyone. Join us at IACP for beverages, giveaways, training, and more!

Visit us at booth #1725

Quantifit® The Gold Standard of Respirator Fit Testing

Within ten seconds of testing, the Quantifit determines if the respirator user has a basic fit. No other quantitative fit test instrument comes close!

Visit us at booth #3808

FLIR Thermal Imaging at IACP

Thermal optics are more affordable than ever. Stop by Booth #4009 and see FLIR's suite of high-performance tactical imagers for yourself.

Visit us at booth #4009

Axon is IN for IACP. Are you?

We'll be showing our latest (and future) technologies, including new AI-powered apps and other products, and unveiling a new campaign.

Visit us at booth #2825

Making It Safer: Collaborating To Advance Officer Safety and Wellness

Award Categories: General Officer Safety, Officers Traffic Safety, Officer Wellness, and Comprehensive Safety. Submit your program today!

Visit us at booth #2403

Making It Safer: A Report on Law Enforcement Fatalities

Did you know that 'Domestic Dispute' calls account for 29% of fatal calls for service? Join as at IACP to see how you can improve your odds!

Visit us at booth #2403

Want Real-Time Access to Over $8 billion in LE Grants?

Powered by PoliceOne and PoliceGrantsHelp, Police GrantFinder is the ultimate law enforcement grant search tool made for you.

Visit us at booth #1448

This message was sent to arthur.somerville@pol.state.ma.us from:

PoliceOne Product Alert | ProductAlerts@policeone.com | Praetorian Digital | 200 Green St Suite 200 | San Francisco, California 94111

Unsubscribe

From: PoliceOne Product Alert
To: Mcdonald, Scott (POL)
Subject: Headed to IACP 2017? Don"t miss these booths.
Date: Tuesday, October 10, 2017 11:12:30 AM

October 10, 2017 | View as webpage

Download the Mobile App

Spillman Flex: Software that Works the Way You Do

What kind of system would your agency build? Spillman Flex provides a flexible, off-the-shelf software solution to support each public safety agency's specific needs and pain points.

Visit us at booth #3037

Preview L3 Mobile Vision's Latest Products at IACP

Get a free T-shirt and a chance to win a set of four Disney park passes when you demo our new Cloud-Based Evidence Management System in our booth at IACP! You don't want to miss this.

Visit us at booth #2549

Still Wasting Your Precious Time and Money?

Dummies Unlimited's proven training products allow your officers to realistically practice de-escalation techniques. Save your agency time and money and reduce liability!

Visit us at booth #3601

Introducing the FATS® 100P: Portable Virtual Training

The lightweight FATS 100P platform features video authoring, judgmental and marksmanship training, and automatic coaching for up to 6 weapons — all in an easily transportable laptop.

Visit us at booth #1909

Don't Miss the Action in IACP Booth 1937!

Experience our new ALPR technologies, engineered to assist with a variety of functions from real-time interdiction to traffic data collection and tolling. Save your agency time and money!

Visit us at booth #1937

Protect Everyone: Demo Our Fully Adjustable Riot Suit

The new Tac Commander™ Riot and Crowd Control Gear is fully adjustable to fit virtually everyone. Join us at IACP for beverages, giveaways, training, and more!

Visit us at booth #1725

Quantifit® The Gold Standard of Respirator Fit Testing

Within ten seconds of testing, the Quantifit determines if the respirator user has a basic fit. No other quantitative fit test instrument comes close!

Visit us at booth #3808

FLIR Thermal Imaging at IACP

Thermal optics are more affordable than ever. Stop by Booth #4009 and see FLIR's suite of high-performance tactical imagers for yourself.

Visit us at booth #4009

Axon is IN for IACP. Are you?

We'll be showing our latest (and future) technologies, including new AI-powered apps and other products, and unveiling a new campaign.

Visit us at booth #2825

Making It Safer: Collaborating To Advance Officer Safety and Wellness

Award Categories: General Officer Safety, Officers Traffic Safety, Officer Wellness, and Comprehensive Safety. Submit your program today!

Visit us at booth #2403

Making It Safer: A Report on Law Enforcement Fatalities

Did you know that 'Domestic Dispute' calls account for 29% of fatal calls for service? Join as at IACP to see how you can improve your odds!

Visit us at booth #2403

Want Real-Time Access to Over $8 billion in LE Grants?

Powered by PoliceOne and PoliceGrantsHelp, Police GrantFinder is the ultimate law enforcement grant search tool made for you.

Visit us at booth #1448

This message was sent to scott.mcdonald@pol.state.ma.us from:

PoliceOne Product Alert | ProductAlerts@policeone.com | Praetorian Digital | 200 Green St Suite 200 | San Francisco, California 94111

Unsubscribe

From: Fenton, Eileen (DOT)
To: Halpin, Michael (POL); Halpin, Michael (POL)
Subject: Hot List Regulations
Date: Thursday, February 2, 2017 10:18:35 AM
Attachments: 700cmr7.pdf

Hi Mike,
As discussed, attached are the regulations that contain the "hot list" language. Please see section 7.02 for definition of hot list, and section 7.05 for hot list data procedure.

Please let me know if you need anything else from me.

Thank you.
Eileen
Eileen M. Fenton
Senior Counsel
Massachusetts Department of Transportation
Ten Park Plaza, Suite 3510
Boston, Massachusetts 02116
T: 857-368-8764
Eileen.Fenton@state.ma.us

From: Mike Sena
To: Mike Sena
Subject: Invitation to 2017 HIDTA Investigative & Intelligence Support Centers, May 9 & 10 San Diego, CA
Date: Friday, April 7, 2017 4:09:56 PM

Dear Partners,

I would like to invite you to the **2017 HIDTA ISC Managers Meeting** that will be held on **Tuesday, May 9 – Wednesday, May 10, 2017**, at the **Westin Hotel** in **San Diego, CA** . This is an opportunity to learn and discuss best practices within Investigative and Intelligence Support Centers and other Field-Based Information Sharing Entities.

Meeting Schedule
Tuesday, May 9, 2017: 8:00 a.m. to 5:00 p.m.
Wednesday, May 10, 2017: 8:00 a.m. to 5:00 p.m.

HOTEL ROOMS MUST BE BOOKED BY NEXT WEEK

Registration Instructions

Log into **https://registration.nhac.org**
Enter the word **Class (case sensitive)** for Username and Password
Select **National HIDTA Assistance Center**
Select **Click to view Meetings Events** link
Select **2016 ISC Managers Meeting**
Fill in the **HOTT Online Application**
Select **Complete Registration**
Once you register, you will receive a letter with hotel and payment information.
Registration Fee: $250.00

Please do not hesitate to call Paul O'Rourke if you have any questions.

Paul J. O'Rourke
Event Coordinator
National HIDTA Assistance Center
1120 N.W. 20th Street, Suite 100
Miami, Florida 33172

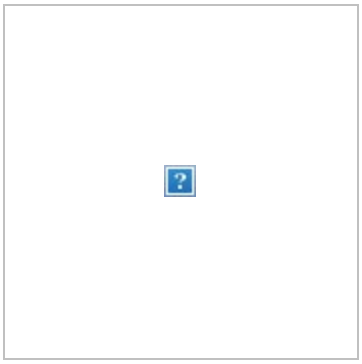
Office Number: 305.715.7600 | Mobile Number: 786.734.0008

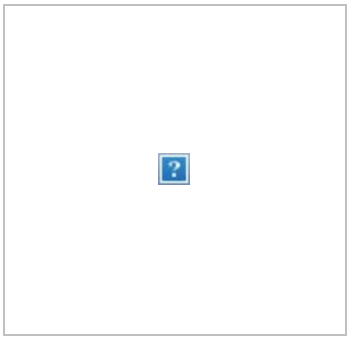
Thank you.

Mike

Mike Sena
Chairman, HIDTA Intelligence Committee
President, NFCA

Director
Northern California High Intensity Drug Trafficking Area
Northern California Regional Intelligence Center
P.O. Box 36102 | San Francisco | CA | 94102
415.725.1000
(24 Hr.) 866.367.8847
msena@ncric.ca.gov





REPORT URGENT THREAT INFORMATION TO THE FBI-JTTF (415) 553-7400
REPORT SUSPICIOUS ACTIVITY TO THE NCRIC www.ncric.org (866) 367-8847

From: Mike Sena
Sent: Tuesday, April 04, 2017 2:27 PM

To: 'ggrimm@sfhidta.org' <ggrimm@sfhidta.org>; 'Douglas Owsley' <Douglas.Owsley@la.hidta.net>; 'Roger Bass' <rbass@la.hidta.net>; 'Samuel Santana' <ssantana@prvihidta.org>; 'Hugo Barrera' <hjbarrera@sflhidta.org>; 'Tony Garcia' <tgarcia@stxhidta.net>; 'Coffey, Andrew F. EOP/ONDCP' <Andrew_F_Coffey@ondcp.eop.gov>; 'fmcdaniel@houstonhidta.net' <fmcdaniel@houstonhidta.net>; 'jmcginty@azhidta.org' <jmcginty@azhidta.org>; 'Frank Fredericks' <ffredericks@rmhidta.org>; 'Jeffrey B. Stamm' <jstamm@midwest-hidta.org>; 'jdaley@pchidta.org' <jdaley@pchidta.org>; 'Daniel V. Moren' <DMoren@nw.hidta.org>; 'wimartin@nhac.org' <wimartin@nhac.org>; ''Fallon, Jay' <jfallon@nehidta.org>; 'Thomas H. Carr' <tcarr@wb.hidta.org>; 'Thomas J. Gorman' <tgorman@rmhidta.org>; 'Robert P. Peryam' <bperyam@nfhidta.org>; ''James F. Bohn' <jbohn@wisconsinhidta.org>; 'Keith Carter' <keithc@lvmpd.com>; 'aaron_kustermann@isp.state.il.us' <aaron_kustermann@isp.state.il.us>; 'Carlos Solano' <carlos.solano@laclear.com>; 'dkennedy@nespin.riss.net' <dkennedy@nespin.riss.net>; 'KENT SHAW' <Kshaw@wsin.riss.net>; 'Kevin.Saupp@HQ.DHS.GOV' <Kevin.Saupp@HQ.DHS.GOV>; 'sarah.chervenak@ic.fbi.gov' <sarah.chervenak@ic.fbi.gov>; 'Lang, Anthony K. (HN) (FBI' <Anthony.Lang@ic.fbi.gov>; 'douglas.w.poole@usdoj.gov' <douglas.w.poole@usdoj.gov>; 'williath@dni.gov' <williath@dni.gov>; 'Mabeus,' <Steven.Mabeus@dni.gov>; 'kerry.sleeper@ic.fbi.gov' <kerry.sleeper@ic.fbi.gov>; 'eboard@nfcausa.org' <eboard@nfcausa.org>; 'Rick Milteer' <rick.milteer@texomahidta.org>; 'Panusky, Daniel' <Daniel.Panusky@usdoj.gov>; 'Ray Massi' <massir@pchidta.org>; 'jagosto@prvihidta.org' <jagosto@prvihidta.org>; 'jwidell@sflhidta.org' <jwidell@sflhidta.org>; 'parduer@gchidta.org' <parduer@gchidta.org>; 'akoffman@milwaukeehidta.org' <akoffman@milwaukeehidta.org>; 'rhoisington@nfhidta.org' <rhoisington@nfhidta.org>; 'bmeredith@milwaukeehidta.org' <bmeredith@milwaukeehidta.org>; 'chense@nfhidta.org' <chense@nfhidta.org>; 'alopez@prvihidta.org' <alopez@prvihidta.org>; 'Leticia Loaiza' <Lloaiza@prvihidta.org>; 'Steve Longsworth' <slongsworth@nw.hidta.org>; 'Luci McKean' <LMcKean@nw.hidta.org>; 'Mark Mathy' <mmathy@milwaukeehidta.org>; 'Mathews, Kim J.' <kmathews@nfhidta.org>; 'Mark.town@sd-lecc.org' <Mark.town@sd-lecc.org>; 'Frank, Roy' <Roy.Frank@sdsheriff.org>; 'Shumaker, Erik' <eshumake@wb.hidta.org>; 'fallon@nehidta.org' <fallon@nehidta.org>; 'Lance Sumpter' <lance.sumpter@texoma.hidta.org>; 'Kean McAdam' <kean.mcadam@sdi.hidta.org>; 'eboard@nfcausa.org'; 'Snyders, Michael R.' <mrsnyders@nhac.org>; 'erasmo.carrizosa@doj.ca.gov' <erasmo.carrizosa@doj.ca.gov>; 'csummers@mi.hidta.net' <csummers@mi.hidta.net>; 'William Castro' <wcastro@mi.hidta.net>; 'Abraham L. Azzam' <aazzam@mi.hidta.net>; 'Kelly, Shannon L. EOP/ONDCP' <shannon_l._kelly@ondcp.eop.gov>; 'cporucznik@lc.hidta.net' <cporucznik@lc.hidta.net>; 'chris.r.gibson@state.or.us' <chris.r.gibson@state.or.us>; 'Hamby, David' <DHamby@achidta.org>; 'joelc@dni.gov' <joelc@dni.gov>; 'Meredith Young' <Meredith.Young@jric.org>; 'Gottlieb, Michael K. EOP/ONDCP' <Michael_K._Gottlieb@ondcp.eop.gov>; Brian M. Rodrigues <brodrigues@ncric.ca.gov>; 'O'Rourke, Paul J.' <pjorourke@nhac.org>; 'Ben Bawden' <bbawden@brooksbawden.com>; 'Ward, Renita' <Renita.Ward@alea.alabama.gov>; 'Trotter, Mike' <Mike.Trotter@alea.alabama.gov>; 'Henry D. Oleyniczak' <HENRYDO@dni.gov>; 'Baldwin, Lesia' <Lesia.Baldwin@alea.alabama.gov>; 'Litaker, Baron' <Baron.Litaker@alea.alabama.gov>; 'Grimm, Gary F' <gfgrimm@sflhidta.org>; Dan Mahoney <dmahoney@ncric.ca.gov>; Karen Sherwood <ksherwood@ncric.ca.gov>; 'Bajwa, Prabhjot S' <Prabhjot.S.Bajwa@usdoj.gov>; 'Pawlowski, Frank' <fpawlowski20@gmail.com>; ''Kenneth Middleton' <kmiddleton@nynjhidta.org>; 'Gardner, Leslie' <Leslie.Gardner@sd-lecc.org>; 'Oregon, Joe' <Joe.Oregon@sd-lecc.org>; 'Mullins, Katherine' <Katherine.Mullins@hq.dhs.gov>; 'Matt McDonald' <mmcdonald@riss.net>; 'john cohen'

<jcohen31@earthlink.net>; 'Laura Cooper' <lcooper@brooksbawden.com>; 'Espana, William A' <waespana@sflhidta.org>; 'chrstina.rogers@doj.ca.gov' <chrstina.rogers@doj.ca.gov>; 'James.E.McDermond@usdoj.gov' <James.E.McDermond@usdoj.gov>; Supervisors <supervisors@ncric.ca.gov>; 'Richard Stanek' <rich.stanek@hennepin.us>; 'jhumphrey@risstech.riss.net' <jhumphrey@risstech.riss.net>; Stephen Gartrell <sgartrell@netsential.com>; 'sgreen@mi.hidta.net' <sgreen@mi.hidta.net>; 'Kshemendra Paul' <kshemendra.paul@gmail.com>
Cc: Alison Yakabe <ayakabe@ncric.ca.gov>; Larry Mack <lmack@ncric.ca.gov>; Rick Weger <rweger@ncric.ca.gov>; 'Dave King (david.king@sdi.hidta.org)' <david.king@sdi.hidta.org>; 'Andy Koffman' <akoffman@northcentralhidta.org>; Diana White <dwhite@ncric.ca.gov>; Craig Buehler <cbuehler@ncric.ca.gov>; 'Chuck McNeal' <Chuck.McNeal@la.gov>; Ken Taylor <ktaylor@ncric.ca.gov>; 'Peter J Dietzman' <Peter.Dietzman@hennepin.us>; 'Kirk, Thomas L' <Thomas.L.Kirk@wv.gov>; 'Alan Rosenhauer' <arosenhauer@risstech.riss.net>; 'Dwight Cunningham' <dcunningham@rmhidta.org>; Jordan Newell <jnewell@ncric.ca.gov>; 'Partridge, Ralph' <Ralph.Partridge@sdi.hidta.org>; 'Boyd, Marigny' <Marigny.Boyd@hq.dhs.gov>; 'Hartzler, Michael L.' <MHartzler@sheriff.hamilton-co.org>; 'Larry Maloney' <lmaloney@risstech.riss.net>; 'Michael Hutton' <mike@mdhtechnology.com>; Elizabeth McCracken <emccracken@ncric.ca.gov>; 'Moseley, Jay' <Jay.Moseley@alea.alabama.gov>; Karen Scott <kscott@ncric.ca.gov>; Jennifer Gragasin <jgragasin@ncric.ca.gov>; 'Martinez, Alberto' <AlbeMart@ociac.ca.gov>; 'Eric Bunde' <Eric.Bunde@laclear.com>; 'Amy Ruiz' <Amy.Ruiz@laclear.ca.gov>; 'Alexander, Robert (USMS)' <Robert.Alexander@usdoj.gov>; Paglino, Marybeth (OTD) (FBI) <Marybeth.Paglino@ic.fbi.gov>; 'Burrows, Mary S. (OTD) (CON) (FBI)' <Mary.Burrows@ic.fbi.gov>; 'Belinda.cumpston@ic.fbi.gov' <Belinda.cumpston@ic.fbi.gov>; 'Chris.knight@ic.fbi.gov' <Chris.knight@ic.fbi.gov>; 'Twyla.strogen@ic.fbi.gov' <Twyla.strogen@ic.fbi.gov>; Stephen Gartrell <sgartrell@netsential.com>
Subject: I&IT Committee: Documents and Contact Information from the March Call

Dear Partners,

Attached are two files, one is the presentation that Alan Rosenhauer gave last Thursday on RISS Identity Management and the other is a list of resources available either on RISSNET or through one of their partners. Alan's contact information is listed below. I've also listed Steve Gartrell's information below for anyone that wants to follow-up with him on his web services offer to provide electronic document tracking markers, membership document distribution management, training services management, Suspicious Activity Report (SAR) collection and other intelligence center web services for $1,700/year. Brian Rodrigues contact information is also below if anyone has questions regarding his single sign on dashboard and identity management project that he is hoping to expand with government and contract data service providers.

<< File: RISS Identity Management Efforts.pptx >> << File: RTSC Quick Reference (RISSNET Resource Availability) 04 03 17.pdf >>

Please help select the next VTC call at: http://doodle.com/poll/6d5nmngqvt724z37. Call in# 201-479-4595;34632758# and meeting URL: http://fuze.me/34632758.

Alan F. Rosenhauer
RISS Chief Technology Officer
Office: 615-849-2576
arosenhauer@risstech.riss.net
RISS Technology Support Center
1639 Medical Center Parkway
Suite 300
Murfreesboro, TN 37179
RISS – A Proven Resource for Law Enforcement™

Stephen Gartrell
Netsential.com, Inc.
12832 Willow Centre Drive
Suite C
Houston, Texas 77066
Email: sgartrell@netsential.com
www.netsential.com
Toll Free: (877) 993-6433 x101
Phone: (281) 631-9900 x101
Mobile: (832) 265-8511

Brian M. Rodrigues
Assistant Deputy Director – IT/Cyber/Risk/ALPR
Northern California Regional Intelligence Center
brodrigues@ncric.ca.gov
415-710-9702

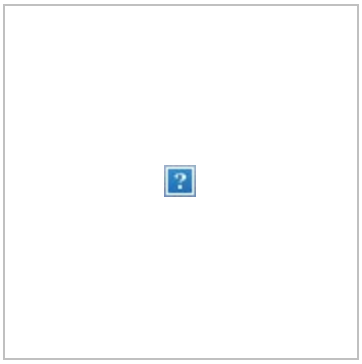
Thank you.

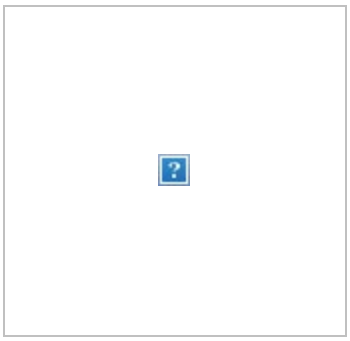
Mike

Mike Sena
Chairman – HIDTA Intelligence Committee
President - National Fusion Center Association

Director
Northern California High Intensity Drug Trafficking Area
Northern California Regional Intelligence Center
P.O. Box 36102 | San Francisco | CA | 94102
415.725.1000
(24 Hr.) 866.367.8847

msena@ncric.ca.gov





REPORT URGENT THREAT INFORMATION TO THE FBI-JTTF (415) 553-7400
REPORT SUSPICIOUS ACTIVITY TO THE NCRIC www.ncric.org (866) 367-8847

From: Mike Sena

Subject: I&IT Committee VTC update/planning w/NDCAC & the Joint IC, DHS & DOJ Inspectors General Report on CT Information Sharing

Good afternoon,

I know sometimes my late West Coast Friday e-mails are at the bottom of Mondays, so I wanted to make sure that you had the selection date poll for this month's call at the top of your virtual box and the notes from last Thursday's call below. I'm also working with are partners at the National Data Communication Assistant Center (NDCAC) to provide an update on the next call regarding their Going Dark data collection surge and the documents attached.

Please help select the next VTC call at: http://doodle.com/poll/6d5nmngqvt724z37. Call in# 201-479-4595;34632758# and meeting URL: http://fuze.me/34632758.

I also wanted to share the attached joint report that was released by the Office of the Director of National Intelligence (ODNI) this past Friday on the Domestic Sharing of Counterterrorism Information. The report is the result of the Inspectors General (IG) of the Intelligence Community (IC), Department of Homeland Security (DHS), and Department of Justice (DOJ) responding to a request from the Senate Select Committee on Intelligence, the Senate Homeland Security and Governmental Affairs Committee, and the Senate Judiciary Committee to conduct a joint review focusing on domestic sharing of counterterrorism information. The report covered our RISS, Fusion Center, PM-ISE, ODNI, NCTC, CICC, DOJ, FBI and DHS partners. The report lacked any discussion regarding the other partners that support the counterterrorism framework such as HIDTAs, EPIC, DEA, and ATF.

<< File: Domestic_Sharing_Counterterrorism_Information_Report.pdf >> << File: STATE AND LOCAL DATA COLLECTION SURGE.DOC >> << File: NDCAC Statistics Collection Tool Device.xlsx >> << File: NDCAC Statistics Collection Tool Device Records Wiretaps.xlsx >>

I look forward to talking with you soon.

Mike

Original Message:

Dear Friends,

I want to thank everyone for their participation in the group and willingness to share their best practices and solutions. Below are the notes from yesterday's call, minus the slide deck from the RISS presentation that will be sent when available. Thank you for the notes Jordan!

The next call will include a presentation on HSIN Exchange from Katie Mullins, update and demonstration of ODMap from the Washington/Baltimore HIDTA, review of the progress on the Michigan HIDTA cyber resiliency/ spear phishing review from Steven Green and Brian Rodrigues, an update on the planning for the in-person meeting in San Francisco the week of September 21st from Paul O'Rourke, and any other items that you would like to cover. We also need to circle back on the ".gov" e-mail discussion in May. Please e-mail me at msena@ncric.ca.gov or text me at 415-725-1000, with any topic suggestions you have for future calls.

We also need support on a task team related to cloud services and a task team for mobile data collection and education platforms. Washington/Baltimore HIDTA Director Tom Carr has volunteered to lead the cloud services task team. To volunteer please contact my executive assistant, Jordan Newell, at jnewell@ncric.ca.gov.

Please go to the following link to help plan the date and time for next month's call: http://doodle.com/poll/6d5nmngqvt724z37.

Thank you again and I look forward to talking with you soon.

Mike

Intelligence & Information Technology Committee and Friends Teleconference
Thursday, March 30, 2017

- **Introduction (Mike Sena)**

  - The goal of this call is to get people together and discuss information sharing projects, best practices, new ideas.
  - Previous call:
    - Cloud technology
    - What's working/what's not?
    - Purchasing: how can we get a better cost with the big box buying power of over 5,000 HIDTA, RISS and Fusion Center members?
    - Using Microsoft 365: remote storage of data.

- **Document Security (Steve Gartrell)**

  - We need technology to track documentation for security purposes. How can we "tag" documents so that if they unfortunately land in the wrong hands there us a mechanism to track down the leak?
  - An example of a tool in place now is when a person registers via the NC HIDTA/NCRIC website, he/she is given a unique identifier. From the web distribution services tool each document stored in a secure area and each document disseminated has the unique identifier on every page of a PDF file being sent out via broadcast email. The identifier can be found at the top and the bottom of the page.
  - Currently, we are working on a mechanism to hide that identifier in plain view, specifically hiding it within the header below the NC HIDTA logo.
  - Documents are automatically locked before they are released to members of the distribution. Members can only print the document.

- ***Mike Sena:*** The National Fusion Center Association is advocating that every fusion center obtains the capability – all HIDTA/RISS centers should as well.
- ***Brian Rodrigues:*** Automation of this system is noteworthy. The identifier is created and assigned automatically.
- General Pricing: $1,700/year includes access to every resource available. Those resources include member registration management, training course management, unique identifier tagging, document library management, and suspicious activity report collection tool. Organizations could lower pricing below $1,700 considerably depending on what your organization needs based on a lower number of tools.
- Steve also does not mind building a prototype in advance for free.
- Always register with agency email. If email bounces back twice, the user is deactivated. This does not delete the user from the system, just deactivates. Also, if an email is forwarded to another non-vetted person, the account will be deactivated if the recipient clicks the no longer interested in receiving the product button.
- Currently working with 40-50 fusion centers.
- All the work is".net", with all of the work being done in house at Netsential.
- For further details go to: http://www.netsential.com/

- **RISS Identity Management Single Sign On (Alan Rosenhauer & Julie Humphrey)**

- The single sign on capabilities creates a world where you don't have to manage multiple passwords, all done by the user through one trusted identity that crosses platforms. The goal is to push the vetting to the organization the user works for and not trying to manage it by an organization that may not understand the rights and privileges that an individual may have in the organization. That way the organization can have better control over its personnel.
- It is designed to make it easier for someone to access multiple sites.
- The next step is to be able to search all content pro-actively. Currently, RISS users can search both RISS and HSIN based on their credentials.
- Looking at including other content providers and become more "Google-like." However, it would not catalog the data like Google does. It would send a live query to provider and the results would depend on the user's profile and permissions.
- A list of connected service providers will be sent out soon.
- ***Hank Olyniczak:*** This project has grown exponentially in recent years. HSIN partnered with EPIC. Now RISS is linked to both portals. This will only continue to grow…

- Kshemendra Paul: As one of the fundamental supporters of the single sign on project when he was Program Manager for the Information Sharing Environment (PM-ISE) and now at DHS he is interested in supporting and helping.
- Bill Martin: How can we have HIDTA's National HIDTA Assistance Center (NHAC) portal connected? Who do we contact? Answer: Alan Rosenhauer at arosenhauer@risstech.riss.net.
- Content Delivery: content delivered based on who you are. One can have everything delivered based on his/her behind the scenes security. Ideally, you wouldn't have to search a bunch of different systems. Let the one system run the queries on your behalf.
- This will limit the need to make multiple accounts. It will "blur the lines" and get users the results the need regardless of what provider it comes from.

  << OLE Object: Picture (Device Independent Bitmap) >>

  Alan Rosenhauer and Kshemendra Paul

- **NCRIC Single Sign On – Regional Level (Brian Rodrigues)**

  - Six connected providers in the initial stages: Internal regional Automated License Plate Reader (ALPR) System, Accurint, Palantir, California Department of Justice's Smart Justice, Vigilant, and Forensic Logic' LEAP.
  - The identity management is connected to what Steve was talking about earlier in that access can be granted to vetted users via their NC HIDTA/NCRIC website registration. Based on roles and pre-authorization we can have user access all these systems at once through their single username, password and two-factor authentication via sms, e-mail or phone and subscription where applicable.
  - Chuck McNeal (LA-SAFE/LSP) Question: Why only six providers?
  - First, this was recently set up. Second, it depends on the willingness of the vendor and to a lot of these companies this is a very new concept. Some companies need to address their limitations before they can jump on board.

    << OLE Object: Picture (Device Independent Bitmap) >>

RFI Exchange/ HSIN Exchange (Katie Mullins)

- Full demo next month. HSIN Exchange currently connects all the 78-designated fusion centers and the Terrorist Screening Center (TSC) for requests for information (RFIs) 24/7 regarding known or suspected terrorists across the US that are contacted by law enforcement or traveling through a port of entry at borders, seaports or airports. It also connects the fusion centers for center to center RFIs.
- HSIN Exchange centralizes RFI's and creates a process management/tracking process that did not exist before for fusion centers or the TSC. Currently pushed out to all fusion centers.
- Welcoming feedback and applying that feedback to future updates.
- Looking at other partners to bring on that contribute to information sharing, including RISS Watch Centers and HIDTA Investigative & Intelligence Support Centers (ISCs).

- **First Two App (Mike Sena)**

  - https://www.firsttwo.com/
  - Goal is to have the most current telephone information. Ideally, a law enforcement official can look at a location and see the most current names and numbers associated with that location. Nothing older than six months.
  - NC HIDTA/NCRIC currently in the trial phase.
  - Pricing:
    - 50 Officers - $200/month
    - 100 officers - $300/month
    - 200 officers - $500/month

- **Mike Sena Comments/Reminders**

  - We need to be proactive on a tactical level and test the security and resilience of our information technology systems as well as all our staff. We cannot afford to be compromised. If we are compromised, we must be able to reduce the risks for all our partners.
  - Identification of vulnerabilities is the key. Last month we discussed NIST standards and the Joe Oregon at the SD-LECC discussed the DHS Cyber Resilience Review: https://www.us-cert.gov/ccubedvp/assessments

- The “Amazing” Abe Azzam, being the outstanding partner that he is, volunteered the Michigan HIDTA for a cyber resiliency review and to conduct a spearphishing review. It will help determine the cyber-age question of will our employees bite? It only takes one!
- Brian Rodrigues and Steven Green’s cyber review work will hopefully be the starting point for creating a continual review and assessment process across the network of field-based intelligence and information sharing entities. Hopefully, we can develop a consistent number of resources nationwide to test each other more efficiently. I know Joe Oregon and several other great partners across are network are standing by to help too.
- ***Need two working groups/tasks teams!***
    1. ***Cloud Technology will be led by Washington Baltimore HIDTA Director Tom Carr***
    2. ***Mobile Collection Platforms – We need at least one volunteer to lead this team.***
- Our next call will include:
    3. HSIN Exchange demonstration and overview.
    4. ODMap updates on the progress of the system and a demonstration
    5. Update on the Michigan HIDTA Cyber Review.
    6. Discussion of the in person meeting currently planned for the week of September 18th in San Francisco, CA.
    7. Anything else that you would like to add….

Mike

-----Original Appointment-----
From: Mike Sena
Sent: Friday, March 24, 2017 3:38 PM

When: Thursday, March 30, 2017 12:00 PM-1:30 PM (UTC-08:00) Pacific Time (US & Canada).
Where: http://fuze.me/34632758 or 201-479-4595;34632758# download for screen sharing: https://www.fuze.com/download and if you don't have a web camera with a microphone or a computer/smart device use 201-479-4595;34632758#

Dear friends,

The High Intensity Drug Trafficking Area (HIDTA) Directors Committee (HDC) requested that I start an IT sub-committee to support the enhancement of best practices for HIDTA cyber security as well as the evaluation and use of technology for the HIDTAs. Our partners at RISS, the fusion centers, EPIC, DOJ, DEA, FBI, ATF and DHS each individually have great resources and ideas that I wanted to bring to the table for the conversation, so I invited a few

friends. Many of them have agreed to join in the discussion and help develop best practices for all our field based intelligence entities. We had our first call last month and the notes from the call are below along with the notes from the January HIDTA Intelligence Committee and Friends call further down.

I also wanted to make sure that everyone was aware of an upcoming technology information data call that all the HIDTA, RISS and fusion center partners should support. Our friends at the National Data Communications Assistance Center (NDCAC) will be conducting a push for agencies to report incidents where encryption hinders investigations. I've attached some older reference documents related to the data being requested. The push is set to begin next week on March 15th. I'll ask Director Marybeth Paglino to send us the current request language and documents to make sure that we are consistently reaching every law enforcement agency in America. They may not all respond, but we want to make sure they know that the NDCAC needs their data.

National HIDTA Assistance Center (NHAC) Director Bill Martin and his right-hand man, Paul O'Rourke, are working to coordinate a face to face meeting for all of us in September in San Francisco. I'll have more details soon.

This call will cover single sign on/identity management, interconnected resource pages for field based intelligence professionals and document dissemination security. Please also look at http://www.policemag.com/channel/technology/articles/2016/09/incident-intel-at-your-fingertips.aspx and https://www.firsttwo.com/. I met with the CEO this week and the platform is very easy to use and I'll add a few comments about it on the call.

<< OLE Object: Picture (Device Independent Bitmap) >>

We will also provide follow-up on a few of the topics listed in the notes below.

I appreciate your willingness to contribute to the cause.

Thank you!

Mike

Information Technology Committee Meeting
February 3, 2017
50 participants

Microsoft 365

In general, most people on this call are content with Microsoft 365 and its abilities in terms of email. Microsoft 365 put together the necessary security needed for government usage with this cloud-based system. Due to the nature of our business, Microsoft 365 US Government was created

through the Azure side. Essentially this allows our information to go through a "secure tunnel" so our information is secure.
Bill Martin brought up four points below that he said Will España could expand on during the next call if needed:

1. Content is logically segregated from customer content in the commercial side.
2. Org customer content is stored within the US
3. Access to org customer content is restricted to screened Microsoft personnel.
4. Office 365 US Government complies with certification and accreditation that are required for US public sector customers. Also complies with Fed RAMP and government guidelines.

Is the hardware physically separate? What's the security like at the data center? Is it physically secure?
CJIS compliancy issues resolved.
Microsoft 365 is good for continuity of business, ability to have a platform that is going to work for your organization in email and any other functionality.
Microsoft 365 provides users the ability to stay operational if something were to happen. We need to have access to important information at all times, and the cloud-base technology provides us with that.
Your fiduciaries dictate whether you get access to the non-profit or government side. Non-profit license has similar security.

-Non-Profit: $4.50 per user which includes downloadable Office.
-Government: Around $8.00 per user.

SharePoint portal service provides the ability for video sharing.
Recommendation: Based on RISS and HIDTA research with the provider, this is the direction we should all go in. The cloud is a benefit to our work and provides the opportunity of continuity of operation and ease of business.

Cyber Security

Our greatest vulnerabilities are our IT systems. One breach in one HIDTA, RISS Center, fusion center affects all the other HIDTAs, RISS Centers and fusion centers across the county. There is a need to implement a type of IT audit to get a reasonable assurance that our internal systems are protected. We want to ensure that we are doing everything we can to prevent a hack. Implement ASAP!
National Guard constructs teams to check their own IT infrastructures. If they were to do this for us, it also builds a relationship with them.
Cyber Resilience Review (CRR) – DHS provides software and will also come out and assist in the conducting an internal audit for your organization. Details are all maintained by DHS and internally. FREE! Joe Oregon provided the link at https://www.us-cert.gov/ccubedvp/assessments

Some concerns included difficulty in coming up with a standard to begin with.

-Start with NIST guidelines. https://www.nist.gov/publications/search?term_node_tid_depth%5B%5D=249421

-Cyber Work Groups within each organization – brainstorm how/where to begin.

-Many subcommittees and other sub-subcommittees with a lack of connectivity between groups working the same or similar topic areas.

-CRR allows you to identify your faults and provides you with suggestions. Also highlights your organization's strengths. In terms of revamping your IT systems, this could be a great

starting point.

Spear Phishing

Using social engineering to get access to data.
Important to provide initial training to partners and internal staff.
Also important to implement spear phishing exercises. Who is your weakest link? Very valuable to test yourselves. (Michigan HIDTA Director Aba Azzam volunteered to have his office trained and tested by the NCHIDTA/NCRIC IT.)

NETI HIDTA Application

IOS/Android App – Free to Download at https://itunes.apple.com/us/app/neti-hidta-identify-emerging-drug-related-threats/id1176394225?mt=8
Educational piece – teaches the user about different types of drugs, toxicity levels, protection, hazards to law enforcement, field test for law enforcement, signs of exposure and symptoms.
Developing a data collection piece soon. The NETI team has also been talking with Prab Bajwa at EPIC regarding data collection platforms.

Drug Monitoring Initiative - Overdose Mapping

Surveillance system for public health.
ODMAP First responders responding to an overdose can press a few buttons and provide data. This data is transferred to a mapping system which tracks overdoses in real time. (Please see the attachments)

-Level 1 User: Enters the data.
-Level 2 User: Can view the map – Police, Fire, Public Health.

The goal is to identify real time overdose spikes and hopefully get public health to take some action.
Being successfully used in two counties in West Virginia. The next step is to get this expanded to all HIDTAs across the country.
This is a responsive website, not an app. Uses location services from the device. The agency using this system determines how they want to display the spikes.

Discussion Points for Future Meetings

Consider a face-to-face meeting. Possibly in San Francisco?
NCITE - App where you can run a complete criminal history check from a cell phone.
Lack of guidance on nationwide retention schedules/purge requirements.
How can we get all HIDTAs switched over to ".gov" accounts?

<< File: ODMAP Spike Analysis_2017_0228.pdf >> << File: ODMap Brochure_Flyer.pdf >> << File: ODMAP User Agreement.docx >> << File: SSL Training Registration Form 2016.pdf >> << File: ODMAP Policies and Procedures 11.21.16.docx >> << File: Overdose Surveillance System.docx >> << File: Regional Introduction to the NDCAC.final.pdf >>

<< File: NDCACStatisticsCollectionTool2016.xlsx >> << File: SOP for Statistics Collection Tool.pdf >> << File: Encryption - Statistical Collection Tool final.pdf >> << File: HSIN-Fact Sheet-HSIN-Intel-v11.pdf >>

Subject: HIDTA Intelligence Committee and Friends Teleconference

Dear friends,

I want to thank everyone that was able to join or send another friend to Monday's call. Below you will find the notes from the call as well as documents that were referenced on the call for your reading pleasure. There are a few action items for your review that are highlighted below. I appreciate your commitment to helping improve our combined information sharing, investigative support and intelligence capabilities.

I look forward to talking with everyone next month.

Mike

HIDTA Intelligence Committee & Friends
January 30, 2017 –
Meeting Notes

Marybeth Paglino, NDCAC Director

- The NDCAC is managed by an executive advisory board that consists of federal, state and local law enforcement members.
- Goal is to put law enforcement in the right direction with technology.
- Free training on the internet, social media exploitation, encryption.
- Large cell site database to assist with cell mapping.
- Technology resource group – almost like a "Help Center."
- Also has a secure website for law enforcement only.
- "Going Dark" – not having the ability to lawfully access technology or data is a major law enforcement issue.
- Statistics Collection Tool: devices that cannot be accessed, companies slow to comply, and ever increasing encrypted data sets have not provided us with enough data to show that there is a problem. NDCAC is trying to collect the data, but they need the entire law enforcement communities' help. Please see the attached letter. HIDTA, RISS and FC Directors are being asked to support the efforts to mobilize collection efforts along with all of the major LE associations.
- In order to access the secure website, law enforcement partners must have LEAP access first.

Kevin Saupp, DHS Office of Intelligence & Analysis

- The Homeland Security Information Network (HSIN) is all about sharing information between

federal, state, local, tribal public safety and homeland security partners and improving cross fusion center, HIDTA, RISS and other field based intelligence entities intelligence and investigative support process coordination. Please see the attached HSIN Fact sheet.

- Facilitate engagement interaction through:

    1. RFI Tool

        - Common template was needed to facilitate a smooth process for the creation, dissemination and collection of requests for information (RFIs) across the country.
        - All fusion centers have access to the system.
        - Goal is to prioritize. Provide a timeline on when your request will be processed, who viewed your request, etc.
        - Security Concerns: HSIN ensured that all data security measures are met and that the individual requestor and responding agency have total control over their data.
        - We are looking for a commitment from the HIDTA Directors to move the Investigative/Intelligence Support Centers (ISCs) into the next group of users. Mike Sena will discuss this at the National HIDTA Directors' Meeting next week.

    2. Application to share production plans

        - Important for de-confliction purposes.
        - Analysts would be able to upload/import their planned production.
        - Ideally this would limit duplicated efforts on the same topics and improve collaboration across field based intelligence entities (Fusion Centers, HIDTA's and RISS Centers) and federal law enforcement intelligence agencies.

Tom Carr, Washington/Baltimore HIDTA Director - Drug Monitoring Initiative and Heroin Response Plan

- Mapping for overdose reports via ESRI platform.
- Implemented in two counties in West Virginia.
- Goal is to track drug overdoses in real time.
- 21 overdose reports (including one fatality) as of last Thursday (1/26).
- Data is collected through law enforcement reporting and Fire/EMS services.
- Ready to roll out in various other locations and a presentation will be made on moving forward to other HIDTAs next week.
- How to implement into GIS environment? Tom Carr, Bryan Costigan, Jay Moseley, and Aaron Kustermann will be connecting to discuss data sharing through the ESRI platform to fusion centers. tcarr@wb.hidta.org; bcostigan@mt.gov; James.Moseley@alea.alabama.gov; aaron_kustermann@isp.state.il.us

Bill Martin, National HIDTA Assistance Center Director and Chris Gibson, Oregon HIDTA Director
NETI – National Emerging Threat Initiative

- Bill Martin, NHAC
- Comparing/contrasting threat assessments from various HIDTA's to develop a smoother capability to provide data to the DEA for the National Drug Threat Assessment.
- Goal is to come up with a core set of questions to allow us to support a national threat assessment.

- Chris Gibson, Oregon HIDTA
    - Analyzing HIDTA's seizure information from 2012-2015.
    - Cocaine becoming an emerging threat.
    - Maybe form a committee to de-conflict efforts and improve the process?
    - Ensure DEA is part of the effort.

FBI Partner Engagement/Training

- FBI interested in providing additional analytical training for analysts.
- Developing a 1-2 week course limited to 50 students sometime in May or June.
- Goal is to have students return to work and coordinate with local FBI field divisions to develop products.
- Next goal is to send analysts to Quantico and train with special agents for the first nine weeks of their training.

Crime Gun Intel Center – ATF

- Partnership with W/B HIDTA that has been very successful in placing ATF analysts in the HIDTA, as where there are drugs there are often times guns and violence associated with subjects using firearms.
- On February 8th from 11:30 am to noon at the 2017 National HIDTA Directors' Meeting, Grand Hyatt, 1000 H St NW, Washington, DC 20001, we will go more in depth on the subject with ATF Assistant Director Jim McDermond and his deputy, John Durastanti, providing the presentation.

Best Practices/Collaborations of HIDTA/RISS/Fusion Centers and collocation with the FBI, DEA and ATF (Mike Sena)

- Last October during a conversation with the FBI Director, Mike Sena discussed developing a presentation on best practices related to collocation and collaboration between all of the field based intelligence entities. Director Comey stated that he would like to have something put together by April for his next SAC meeting.

Hopefully we can get a rough draft together before next month's call.

Technology Subcommittee Development – VTC this Friday, February 3rd at 1pm Pacific/4pm Eastern (Mike Sena)

- We need to provide recommendations for MS Office 365.
- Plan to discuss cyber defense and security for networks.
- We need to test networks and make sure analysts and other HIDTA, RISS and FC employees can recognize spear phishing, social engineering attack methodologies and are familiar with cyber security protocol and practices.

From: Robert McConnell
To: All ASCIA Members
Cc: Ben Bawden; Ron Brooks
Subject: License Plate Reader - Policy Development Template
Date: Tuesday, February 7, 2017 11:03:03 PM
Attachments: LPR Policy Template FINAL 2-7-17.pdf

All ASCIA Members,
Attached is the newly released License Plate Reader Policy Development Template produced by BJA.

This document was developed through a collaborative partnership among the associations represented on the Criminal Intelligence Coordinating Council (CICC), the U.S. Department of Homeland Security, the Bureau of Justice Assistance, and numerous federal, state, and local partners. CICC is chaired by Director Vernon Keenan, Georgia Bureau of Investigation. ASCIA representative on the CICC is Director Mark Gwyn, Tennessee Bureau of Investigation. Several ASCIA members were part of the working group that developed this template.

This documents is also available online at: https://it.ojp.gov/GIST/1197/License-Plate-Reader-Policy-Development-Template-for-Use-in-Intelligence-and-Investigative-Activities

Bob

Robert McConnell
Executive Director
Association of State Criminal Investigative Agencies (ASCIA)
Cell: (561) 239-1345
Email: Executive.Director@ascia.org
www.ascia.org

This e-mail transmission and any attachments may contain information that is proprietary, privileged and/or confidential and is intended exclusively for the person(s) to whom it is addressed. Any use, copying, retention, or disclosure by any person other than the intended recipient or the intended recipient's designees is strictly prohibited. If you are not the intended recipient or their designee, please notify the sender immediately by return e-mail and delete all copies.

From: Egnitz, Brian (POL)
To: Mason, Christopher (POL)
Cc: Quinn, Dermot (POL)
Subject: LPR Options
Date: Wednesday, March 29, 2017 9:29:29 AM
Attachments: Plate Alert brochure.pdf

Please see some ALPR options below.

If ALPRs are deployed similar to what we did in Sturbridge, DFS benefits as well as DIS. We created a custom email group for the barracks and loaded a custom hotlist. If partnered with DHQ with BOLO Roll Call they can push their own hotlist into the reader (this has better auditing than BOSS). SP Sturbridge have had a couple of seizures and stolen recovered because of the reader stationed on 84.

Also included below is Plate Alert with analysis package. I've include the brochure

Option A (30 LPRs)				
	Type	Quantity	Cost	Sub Total
	Truck	[redacted]		$ 58,256.00
	LPR			$ 357,570.00
	Trailer			$ 521,550.00
Fixed/Reoccurring Costs	Server upgrade			$ 29,365.77
Fixed/Reoccurring Costs	Software update			$ 62,040.00
Fixed/Reoccurring Costs	Verizon			$ 18,000.00
				$ 1,046,781.77

Option B (20 LPRs)				
	Type	[redacted]		Sub Total
	Truck			$ 58,256.00
	LPR			$ 238,380.00
	Trailer			$ 347,700.00
Fixed/Reoccurring Costs	Server upgrade			$ 29,365.77
Fixed/Reoccurring Costs	Software update			$ 62,040.00
Fixed/Reoccurring Costs	Verizon			$ 12,000.00
				$ 747,741.77

Option C (10 LPRs)				
	Type	Quantity	Cost	Sub Total
	Truck	[redacted]		$ 58,256.00
	LPR			$ 119,190.00
	Trailer			$ 173,850.00

Fixed/Reoccurring Costs	Server upgrade	[redacted]	$ 29,365.77
Fixed/Reoccurring Costs	Software update		$ 62,040.00
Fixed/Reoccurring Costs	Verizon		$ 6,000.00
			$ 448,701.77

From: Egnitz, Brian (POL)
Sent: Friday, March 24, 2017 2:14 PM
To: Mason, Christopher (POL)
Cc: Quinn, Dermot (POL)
Subject: ALPR Quote

Please find the attached quotes for 30 LPRs and 30 Solar Trailers. I'm still waiting on a quote for 2 4x4 trucks.

Total LPR $419,610
Total Trailer $508,400.00
Server Upgrade $29,365.77
Total Cost $957,357.77 + 2 4x4 trucks $ TBD

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
978-451-3710 (Maynard)
508-988-7216 (GHQ)

From: Egnitz, Brian (POL)
To: Quinn, Dermot (POL)
Subject: LPR Options
Date: Thursday, June 22, 2017 2:39:48 PM
Attachments: Plate Alert brochure.pdf
ATT00001.htm

Please see some ALPR options below.

If ALPRs are deployed similar to what we did in Sturbridge, DFS benefits as well as DIS. We created a custom email group for the barracks and loaded a custom hotlist. If partnered with DHQ with BOLO Roll Call they can push their own hotlist into the reader (this has better auditing than BOSS). SP Sturbridge have had a couple of seizures and stolen recovered because of the reader stationed on 84.

Also included below is Plate Alert with analysis package. I've include the brochure

Option A (30 LPRs)				
	Type	Quantity	Cost	Sub Total
	Truck	[redacted]		$ 58,256.00
	LPR			$ 357,570.00
	Trailer			$ 521,550.00
Fixed/Reoccurring Costs	Server upgrade			$ 29,365.77
Fixed/Reoccurring Costs	Software update			$ 62,040.00
Fixed/Reoccurring Costs	Verizon			$ 18,000.00
				$ 1,046,781.77

Option B (20 LPRs)				
	Type	Quantity	Cost	Sub Total
	Truck	[redacted]		$ 58,256.00
	LPR			$ 238,380.00
	Trailer			$ 347,700.00
Fixed/Reoccurring Costs	Server upgrade			$ 29,365.77
Fixed/Reoccurring Costs	Software update			$ 62,040.00
Fixed/Reoccurring Costs	Verizon			$ 12,000.00
				$ 747,741.77

Option C (10 LPRs)				
	Type	Quantity	Cost	Sub Total
	Truck	[redacted]		$ 58,256.00
	LPR			$ 119,190.00
	Trailer			$ 173,850.00
Fixed/Reoccurring Costs	Server upgrade			$ 29,365.77

Fixed/Reoccurring Costs	Software update	G.L. c. 4 sec. 7 cl 26 (n)(security); G.L. c. 4 sec. 7 cl 26(f)(investigat	$ 62,040.00
Fixed/Reoccurring Costs	Verizon		$ 6,000.00
			$ 448,701.77

From: Egnitz, Brian (POL)
Sent: Friday, March 24, 2017 2:14 PM
To: Mason, Christopher (POL)
Cc: Quinn, Dermot (POL)
Subject: ALPR Quote

Please find the attached quotes for 30 LPRs and 30 Solar Trailers. I'm still waiting on a quote for 2 4x4 trucks.

Total LPR $419,610
Total Trailer $508,400.00
Server Upgrade $29,365.77
Total Cost $957,357.77 + 2 4x4 trucks $ TBD

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
978-451-3710 (Maynard)
508-988-7216 (GHQ)

From: Quinn, Dermot (POL)
To: Halpin, Michael (POL)
Cc: Hughes, Francis P (POL) (francis.hughes@MassMail.State.MA.US)
Subject: lpr policies
Date: Friday, February 3, 2017 2:50:00 PM
Attachments: TRF-11 Automatic License Plate Recognition New 7-22-2014.pdf
ALPR Law Enforcement Dept Model Policy - Final 20131008 (1).pdf
image001.png

Mike,

The DS ask that I forward these LPR policies to you re our meeting with DOT.

Have a great weekend.

Dermot

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Investigative Services
Massachusetts State Police

From:	Jay.Scheck@thomsonreuters.com
To:	Barton, Shannan (POL); Bender, Sean (POL); Bois, Marcy (POL); Foley, Kristine (POL); Huchowski, James (POL); Huchowski, kerra (POL); Iwanicki, Richard (POL); Mores, Frank; Newton, Justin (POL); lindsey.nustrom@massmail.state.ma.us; sj.oleary@state.ma.us; shawn.oneil@state.ma.us; laurie.panocopolous@state.ma.us; Pinkes, William (POL); Pirrotta, Melissa (POL); Sojka, Robert (POL); Matthew.Thomas@thomsonreuters.com; Pinkes, William (POL); Luggelle, Mark (POL)
Cc:	Panacopoulos, Laurie (POL); Matthew.Thomas@thomsonreuters.com
Subject:	LPR Success Stories on CLEAR
Date:	Thursday, November 2, 2017 1:22:31 PM
Attachments:	Why Take Our Word For It.pdf

Hi all, the trial of LPR is wrapping up and I'm looking forward to getting your feedback and any success stories.

Here are few of my own:

- This morning I was up at the Essex County DA's office and we ran a grid search on a murder that took place in Lawrence, the LPR truck had 21 plates within a block of the murder, within an hour of when the murder took place. List of possible witnesses.

- Connecticut Dept of Corrections found a guy they'd been trying to find for over three years and that was just in the first day of having access to the LPR data in CLEAR.

I attached a few more success stories from around the country.

Let us know how it's going!

All the best,
Jay

Jay Scheck
Government Account Executive – Investigative Solutions

THOMSON REUTERS the answer company

Cell: 617.963.4488 / Email: jay.scheck@tr.com
LinkedIn: www.linkedin.com/in/jayscheck/

New England Office:

22 Thomson Place
Boston, MA 02210

Manage your email marketing preferences here.

From: Dunne, Michaela (CHS)
To: Dunne, Michaela (CHS)
Cc: Hutchinson, Daniel (CHS)
Subject: Nlets Training PowerPoint Presentation
Date: Friday, November 3, 2017 11:41:27 AM
Attachments: Nlets Training for Massachusetts - 11.01.17.pptx

---

Good Morning,

Thank you to all who were able attend the Nlets training on November 1. We hope that you and/or your staff found the information to be helpful.

I have attached the PowerPoint presentation to this email. Please forward to your staff that attended the training, or anyone who was unable to attend but may find the information useful. This has also been uploaded to the DCJIS Extranet (only accessible via computers with access to CJIS) under the "Documents and Manuals" tab: http://170.154.225.103/default.aspx.

As always, if you have any questions about the Nlets transactions covered at the training, or any other CJIS related questions, do not hesitate to contact the CJIS Support Services Unit at 617.660.4710 or via email at cjis.support@state.ma.us.

Thank you,

Michaela Dunne | Manager of Law Enforcement & Justice Services
Massachusetts Department of Criminal Justice Information Services
200 Arlington Street, Suite 2200
Chelsea, MA 02150
p. 617.660.4682 | f. 617.884.4601
michaela.dunne@state.ma.us | mass.gov/cjis

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: Ardizzoni, Alyssa (CHS)
Sent: Thursday, October 26, 2017 11:11 AM
ToCc: Hutchinson, Daniel (CHS); Dunne, Michaela (CHS)
Subject: Reminder: Nlets Training Announcement - November 1, 2017

Good Morning,

The Department of Criminal Justice Information Services (DCJIS) is pleased to host Ms. Teri Fournier-Harsin, Nlets Training Manager, for a comprehensive Nlets training on November 1. This training will

cover topics including the importance of nationwide information sharing as well as overviews of many of the specific Nlets queries available for law enforcement officers and personnel through the Massachusetts Criminal Justice Information System (CJIS).

This training is open to all CJIS Representatives and any other officer or employee who currently utilizes the Nlets queries through CJIS. There is no cost to attend this training.

DATE: Wednesday, November 1
TIME: 9:00am to 2:00pm
LOCATION: Kowloon Restaurant
948 Broadway
Saugus, MA 01906

Pre-registration is required on the DCJIS Extranet: http://170.154.225.103/trainingannouncements1/default.aspx. You need to be using a computer that has access to the CJIS System to access this link.

For additional information, please call the CJIS Support Services Unit at 617.660.4710.

Sincerely,

Alyssa Ardizzoni | CJIS Representative
Massachusetts Department of Criminal Justice Information Services
CJIS Support Services
200 Arlington Street, Suite 2200
Chelsea, MA 02150
t: 617.660.4711| f: 617.884.4601
Alyssa.ardizzoni@state.ma.us| http://www.mass.gov/cjis

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: Sales PIPS
To: Egnitz, Brian (POL)
Subject: Pending ALPR Opportunities
Date: Thursday, November 30, 2017 5:44:05 PM
Attachments: P492 Fixed Camera + Plate Alert Software_V2.pdf
ALPR Customer Letter Neology 11_1_17.pdf
Neology W9 form.pdf

Good afternoon,

Just a quick email regarding the existing quotes that your department currently has pending with our ALPR division.
Recently we were acquired by Neology, and are no longer with 3M. We quickly took back our PIPS TECHNOLOGY name and brand.
We are very excited to continue our business with you and wanted to provide the new email address and phone number for support regarding your existing orders.

Please find our Customer letter, Company W9 and your pending orders that sales had worked with your department on.
If you would like these prices transferred to Neology documents, please email me anytime for assistance.

I look forward in hearing from you.
Kind Regards

PIPS TECHNOLOGY - A Neology Business
Miranda Fischer
ALPR Sales
833-PIPS-LPR Opt. 1 (833-747-7577)
sales@pipstechnology.com

From: PoliceGrantsHelp eNews
To: Conneely, Paul (POL)
Subject: Police grant advice: Preventing and preparing for school mass casualty; How spectrometers can aid crime scene investigations
Date: Friday, October 20, 2017 3:06:27 PM

October 20, 2017 | View as webpage

Ask a Grant Expert

Dear PoliceGrantsHelp Member,

In this month's eNews, Judy Riffle, P1 Contributor, talks about what you need to know to prepare and win school emergency preparedness grants. While Linda Gilbertson covers how spectrometers play a major role in the current criminal justice system and how agencies can purchase the devices with grant funding.

Are you going to the IACP conference in Philadelphia this week? We are! Sarah Wilson and Carrie Schneider will be there along with the rest of the Praetorian Digital family, so come by with your grant questions or just stop by to say "Hello"! We will be at **PoliceOne.com - Praetorian Digital Booth #1448**. We hope to see you there!

— *The PoliceGrantsHelp Team*

FEATURED ARTICLE

Police grant advice: Preventing and preparing for school mass casualty

By Judy Riffle, P1 Contributor

Here's what you need to know to prepare and win school emergency preparedness grants

Introducing the FATS® 100P Virtual Training System. Portable. Easy to Operate.

Ask About Grant Assistance at Leonardo's IACP Booth 1937

Leonardo is working with



The lightweight FATS 100P features video authoring, judgmental and marksmanship training, enhanced UUI, automatic coaching, 360° sound board and supports up to 6 weapons–in an easily transportable laptop.

The future of virtual training



PGH to bring you services and guidance related to the grant-assisted procurement of our force-multiplying ALPR technologies. Please stop by IACP **booth #1937** for details.

Get grant assistance

GET GRANT ASSISTANCE

PoliceGrantsHelp offers customized grant assistance in several categories. Click on the links below to access free grant services including: research, consulting and application assistance.

- AEDs
- Armored Vehicles
- Boats
- Crime Analysis and Investigation Software
- Explosives Detection
- Forensic 3D Laser Scanners
- Less Lethal
- Manned Mobile Surveillance
- Mobile Forensics
- Online Training
- Radiation Detection
- Specialty Vehicles
- Thermal Cameras (EO/IR)
- Training Simulation
- X-Ray Body Scanner
- Airborne Surveillance
- Biometric Identification
- Body Cameras
- Digital Investigation Software
- Firearms Training
- In Car Video
- License Plate Readers
- Mobile Command Centers
- Narcotics Identification
- Police Motorcycles
- Radios
- Tablets
- Traffic Management Solutions
- Use of Force Software

ALL GRANTS HELP

POLICEGRANTSHELP EXCLUSIVE

How spectrometers can aid crime scene investigations

By Linda Gilbertson

MORE GRANTS NEWS

DOJ: 4 cities may have sanctuary city violations

Grants awarded to Okla. tribes for public



As spectrometers are included in FEMA's Authorized Equipment List, agencies can purchase the devices with grant funding

More

safety efforts

DOJ awards nearly $59M to fight opioid epidemic, fund drug courts

Aftermath services launches 6th annual K-9 grant

All Grant News

Get Free Grant Help for Police Narcotics Identification Products



B&W Tek has partnered with our grant experts to offer your department free grant assistance for police narcotics identification products.

Request free help today

UPCOMING GRANTS

Grant	Grant Deadline
Homeland Security Grant Program (HSGP California)	11/01/2017
Byrne Justice Assistance Grant (JAG Virginia)	11/03/2017
Enhanced Training and Services to End Abuse in Later Life Program	11/08/2017
Georgia Association of Women Lawyers Grants	11/20/2017
DUI Enforcement Equipment Grant - Utah	11/30/2017
Firehouse Subs Public Safety Foundation Grants	11/30/2017
APS Community Giving	11/30/2017
Energy/Mineral Impact Assistance Fund (EIAF Colorado)	12/01/2017
Edward Byrne Memorial Justice Assistance Grant (JAG) (California)	12/01/2017
STOP Violence Against Women Formula Grant (VAWA Maine)	12/06/2017

Interested in finding more grant opportunities

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

This message was sent to paul.conneely@massmail.state.ma.us from:

PoliceGrantsHelp eNews | Newsletter@PoliceOne.com | Praetorian Digital | 200 Green St Suite 200 | San Francisco, California 94111

Unsubscribe

From: PoliceGrantsHelp eNews
To: Silva, Patrick (POL)
Subject: Police grant advice: Preventing and preparing for school mass casualty; How spectrometers can aid crime scene investigations
Date: Friday, October 20, 2017 3:06:29 PM

October 20, 2017 | View as webpage

Ask a Grant Expert

Dear PoliceGrantsHelp Member,

In this month's eNews, Judy Riffle, P1 Contributor, talks about what you need to know to prepare and win school emergency preparedness grants. While Linda Gilbertson covers how spectrometers play a major role in the current criminal justice system and how agencies can purchase the devices with grant funding.

Are you going to the IACP conference in Philadelphia this week? We are! Sarah Wilson and Carrie Schneider will be there along with the rest of the Praetorian Digital family, so come by with your grant questions or just stop by to say "Hello"! We will be at **PoliceOne.com - Praetorian Digital Booth #1448**. We hope to see you there!

— *The PoliceGrantsHelp Team*

FEATURED ARTICLE

Police grant advice: Preventing and preparing for school mass casualty

By Judy Riffle, P1 Contributor

Here's what you need to know to prepare and win school emergency preparedness grants

Introducing the FATS® 100P Virtual Training System. Portable. Easy to Operate.

Ask About Grant Assistance at Leonardo's IACP Booth 1937

Leonardo is working with



The lightweight FATS 100P features video authoring, judgmental and marksmanship training, enhanced UUI, automatic coaching, 360° sound board and supports up to 6 weapons–in an easily transportable laptop.

The future of virtual training



PGH to bring you services and guidance related to the grant-assisted procurement of our force-multiplying ALPR technologies. Please stop by IACP **booth #1937** for details.

Get grant assistance

GET GRANT ASSISTANCE

PoliceGrantsHelp offers customized grant assistance in several categories. Click on the links below to access free grant services including: research, consulting and application assistance.

- AEDs
- Armored Vehicles
- Boats
- Crime Analysis and Investigation Software
- Explosives Detection
- Forensic 3D Laser Scanners
- Less Lethal
- Manned Mobile Surveillance
- Mobile Forensics
- Online Training
- Radiation Detection
- Specialty Vehicles
- Thermal Cameras (EO/IR)
- Training Simulation
- X-Ray Body Scanner
- Airborne Surveillance
- Biometric Identification
- Body Cameras
- Digital Investigation Software
- Firearms Training
- In Car Video
- License Plate Readers
- Mobile Command Centers
- Narcotics Identification
- Police Motorcycles
- Radios
- Tablets
- Traffic Management Solutions
- Use of Force Software

ALL GRANTS HELP

POLICEGRANTSHELP EXCLUSIVE

How spectrometers can aid crime scene investigations

By Linda Gilbertson

MORE GRANTS NEWS

DOJ: 4 cities may have sanctuary city violations

Grants awarded to Okla. tribes for public



As spectrometers are included in FEMA's Authorized Equipment List, agencies can purchase the devices with grant funding

More

safety efforts

DOJ awards nearly $59M to fight opioid epidemic, fund drug courts

Aftermath services launches 6th annual K-9 grant

All Grant News

Get Free Grant Help for Police Narcotics Identification Products



B&W Tek has partnered with our grant experts to offer your department free grant assistance for police narcotics identification products.

Request free help today

UPCOMING GRANTS

Grant	Grant Deadline
Homeland Security Grant Program (HSGP California)	11/01/2017
Byrne Justice Assistance Grant (JAG Virginia)	11/03/2017
Enhanced Training and Services to End Abuse in Later Life Program	11/08/2017
Georgia Association of Women Lawyers Grants	11/20/2017
DUI Enforcement Equipment Grant - Utah	11/30/2017
Firehouse Subs Public Safety Foundation Grants	11/30/2017
APS Community Giving	11/30/2017
Energy/Mineral Impact Assistance Fund (EIAF Colorado)	12/01/2017
Edward Byrne Memorial Justice Assistance Grant (JAG) (California)	12/01/2017
STOP Violence Against Women Formula Grant (VAWA Maine)	12/06/2017

Interested in finding more grant opportunities

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

This message was sent to patrick.silva@pol.state.ma.us from:

PoliceGrantsHelp eNews | Newsletter@PoliceOne.com | Praetorian Digital | 200 Green St Suite 200 | San Francisco, California 94111

Unsubscribe

From: Mason, Christopher (POL)
To: Mason, Christopher (POL)
Subject: Power Core Template.pptx
Date: Thursday, April 6, 2017 5:02:00 PM
Attachments: Power Core Template.pptx

From: Mason, Christopher (POL)
To: Mason, Christopher (POL)
Subject: Power Core Template.pptx
Date: Wednesday, April 5, 2017 5:05:00 PM
Attachments: Power Core Template.pptx

From: Mason, Christopher (POL)
To: Mason, Christopher (POL)
Subject: Power Core Template.pptx
Date: Friday, April 7, 2017 10:54:39 AM
Attachments: Power Core Template.pptx

From: Griffin, Daniel (POL)
To: Daniel Griffin (knightpro@comcast.net)
Subject: ppt
Date: Friday, October 27, 2017 1:03:59 PM
Attachments: Automated License Plate Reader.ppt
TRF-11 Automatic License Plate Recognition 11-25-2013 FINAL DRAFT.doc
PA PowerPoint Slide.pdf
image001.png

Lieutenant Daniel J. Griffin 1129
Massachusetts State Police
Traffic Programs Section
General Headquarters
480 Worcester Rd. **(please note new address)**
Framingham, Ma. 01702
508-988-7404
daniel.griffin@massmail.state.ma.us

From: Egnitz, Brian (POL)
To: Pouliot, Peter P 1SG USARMY NG MAARNG (US)
Subject: RE: CopLink
Date: Friday, June 30, 2017 7:49:00 AM

Hi Pete,

How are we making out on funding?

-Brian

From: Egnitz, Brian (POL)
Sent: Wednesday, May 10, 2017 11:32 AM
To: 'peter.p.pouliot.mil@mail.mil'
Cc: Quinn, Dermot (POL); Mason, Christopher (POL); Sojka, Robert (POL)
Subject: CopLink

Hi Pete,

Per your request, here are some of the CopLink projects that we need funded.

Thanks, Brian

CopLink Enhancements

Project Description:

The Commonwealth of Massachusetts's Fusion Center hosts IBM i2 COPLINK for Local, State and Federal law enforcement agencies. IBM i2 COPLINK is police investigation software that consolidates data from many sources, aids collaboration and helps generate tactical leads quickly. CopLink is used to search record management systems, registry data and criminal history records to solve various crime, such as Homicides, Drug Trafficking and Bank Robberies. This tool provides advanced analytics to law enforcement, data exchange and interoperability to improve connectivity between information sharing systems.

Scope of Work

1. Map the Boston Police Departments Record Management System into CopLink ($28,300)
2. Map the MBTA (Massachusetts Bay Transit Authority) Police Records System into CopLink. ($18,800)
3. Map Lawrence Police Department Record Management System into CopLink (est. $25,000)
4. Map Board of Probation data into CopLink ($22,400)
5. Enhance CopLink to show RMV (Registry of Motor Vehicles) driver's license photos inside of the CopLink software ($63,760)

6. Map the States Automated License Plate Reader Database into CopLink (est. $30,000)
7. Map the States Electronic Citation Database (Civil Motor Vehicle Citation) ($19,850)

Definitions:

A records management system (RMS) is “an agency-wide system that provides for the storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, or files pertaining to law enforcement operations. RMS covers the entire life span of records development—from the initial generation to its completion. An effective RMS allows single entry of data, while supporting multiple reporting mechanisms.” (This definition is taken from both the Bureau of Justice Assistance’s Standard Functional Specifications for Law Enforcement Records Management Systems and the International Association of Chiefs of Police [IACP]/Department of Justices’ Community Oriented Policing Services [COPS] Technology Technical Assistance Program’s Records Management Systems documents.)

“Records” are the information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business. The International Council on Archives (ICA) Committee on Electronic Records defines a record as, “recorded information produced or received in the initiation, conduct or completion of an institutional or individual activity and that comprises content, context and structure sufficient to provide evidence of the activity.”

BOP database contains Criminal Offender Record Information, which consists of records and data in any communicable form compiled by a Massachusetts criminal justice agency about an identifiable individual that relate to:

- Nature or disposition of a criminal charge,
- An arrest,
- A pre-trial proceeding,
- Other judicial proceedings,
- Sentencing,
- Incarceration,
- Rehabilitation,
- Release

Automated License Plate Recognition (ALPR) is a technology that uses optical character recognition (OCR) to automatically read license plate characters.

There are two types of ALPR: stationary, which uses infrared (IR) cameras at high fixed points, and mobile, which uses vehicle-mounted IR cameras.

Stationary cameras can be mounted on signs, street lights, highway overpasses or buildings as a cost-effective way to monitor moving and parked vehicles twenty-four hours a day. Camera software is able to identify the pixel patterns that make up a license plate and translate the letters and numbers on the plate to a digital format. The plate data is then

sent to a database where it is compared in real-time to a list of plate numbers that belong to "vehicles of interest". If the system detects a match, it sends an alert to the dispatcher or other designated personnel.

Mobile ALPR software suites use multiple cameras mounted on a vehicle. As the vehicle moves, it photographs license plates and transmits plate data to a database. The database may be a national database or it may be created at the local level and downloaded into the vehicle's onboard computer at the beginning of each shift. If the system detects a match, the officer receives an alert on his computer. A mobile ALPR can read up to 1,000 plates per hour and cover two or more lanes of traffic at once.

Automated License Plate Recognition has many uses including:
•Recovering stolen cars.
•Identifying drivers with an open warrant for arrest.
•Catching speeders by comparing the average time it takes to get from stationary camera A to stationary camera B.
•Determining what cars do and do not belong in a parking garage.
•Expediting parking by eliminating the need for human confirmation of parking passes.

ALPR is known by several other names, including Automatic Number Plate Recognition (ANPR), Automatic Vehicle Identification (AVI), Car Plate Recognition (CPR), License Plate Recognition (LPR), and Lecture Automatique de Plaques d'Immatriculation (LAPI).

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7216 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

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

From: Egnitz, Brian (POL)
To: Pouliot, Peter P 1SG USARMY NG MAARNG (US)
Subject: RE: CopLink
Date: Monday, July 17, 2017 11:26:00 AM

I spoke to IBM regarding contract info, let me know when we can set up a meeting to discuss.

From: Egnitz, Brian (POL)
Sent: Friday, June 30, 2017 7:49 AM
To: Pouliot, Peter P 1SG USARMY NG MAARNG (US)
Subject: RE: CopLink

Hi Pete,

How are we making out on funding?

-Brian

From: Egnitz, Brian (POL)
Sent: Wednesday, May 10, 2017 11:32 AM
To: 'peter.p.pouliot.mil@mail.mil'
Cc: Quinn, Dermot (POL); Mason, Christopher (POL); Sojka, Robert (POL)
Subject: CopLink

Hi Pete,

Per your request, here are some of the CopLink projects that we need funded.

Thanks, Brian

CopLink Enhancements

Project Description:

The Commonwealth of Massachusetts's Fusion Center hosts IBM i2 COPLINK for Local, State and Federal law enforcement agencies. IBM i2 COPLINK is police investigation software that consolidates data from many sources, aids collaboration and helps generate tactical leads quickly. CopLink is used to search record management systems, registry data and criminal history records to solve various crime, such as Homicides, Drug Trafficking and Bank Robberies. This tool provides advanced analytics to law enforcement, data exchange and interoperability to improve connectivity between information sharing systems.

Scope of Work

1. Map the Boston Police Departments Record Management System into CopLink ($28,300)
2. Map the MBTA (Massachusetts Bay Transit Authority) Police Records System into

CopLink. ($18,800)
3. Map Lawrence Police Department Record Management System into CopLink (est. $25,000)
4. Map Board of Probation data into CopLink ($22,400)
5. Enhance CopLink to show RMV (Registry of Motor Vehicles) driver's license photos inside of the CopLink software ($63,760)
6. Map the States Automated License Plate Reader Database into CopLink (est. $30,000)
7. Map the States Electronic Citation Database (Civil Motor Vehicle Citation) ($19,850)

Definitions:

A records management system (RMS) is "an agency-wide system that provides for the storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, or files pertaining to law enforcement operations. RMS covers the entire life span of records development—from the initial generation to its completion. An effective RMS allows single entry of data, while supporting multiple reporting mechanisms." (This definition is taken from both the Bureau of Justice Assistance's Standard Functional Specifications for Law Enforcement Records Management Systems and the International Association of Chiefs of Police [IACP]/Department of Justices' Community Oriented Policing Services [COPS] Technology Technical Assistance Program's Records Management Systems documents.)

"Records" are the information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business. The International Council on Archives (ICA) Committee on Electronic Records defines a record as, "recorded information produced or received in the initiation, conduct or completion of an institutional or individual activity and that comprises content, context and structure sufficient to provide evidence of the activity."

BOP database contains Criminal Offender Record Information, which consists of records and data in any communicable form compiled by a Massachusetts criminal justice agency about an identifiable individual that relate to:

- Nature or disposition of a criminal charge,
- An arrest,
- A pre-trial proceeding,
- Other judicial proceedings,
- Sentencing,
- Incarceration,
- Rehabilitation,
- Release

Automated License Plate Recognition (ALPR) is a technology that uses optical character recognition (OCR) to automatically read license plate characters.

There are two types of ALPR: stationary, which uses infrared (IR) cameras at high fixed

points, and mobile, which uses vehicle-mounted IR cameras.

Stationary cameras can be mounted on signs, street lights, highway overpasses or buildings as a cost-effective way to monitor moving and parked vehicles twenty-four hours a day. Camera software is able to identify the pixel patterns that make up a license plate and translate the letters and numbers on the plate to a digital format. The plate data is then sent to a database where it is compared in real-time to a list of plate numbers that belong to "vehicles of interest". If the system detects a match, it sends an alert to the dispatcher or other designated personnel.

Mobile ALPR software suites use multiple cameras mounted on a vehicle. As the vehicle moves, it photographs license plates and transmits plate data to a database. The database may be a national database or it may be created at the local level and downloaded into the vehicle's onboard computer at the beginning of each shift. If the system detects a match, the officer receives an alert on his computer. A mobile ALPR can read up to 1,000 plates per hour and cover two or more lanes of traffic at once.

Automated License Plate Recognition has many uses including:
•Recovering stolen cars.
•Identifying drivers with an open warrant for arrest.
•Catching speeders by comparing the average time it takes to get from stationary camera A to stationary camera B.
•Determining what cars do and do not belong in a parking garage.
•Expediting parking by eliminating the need for human confirmation of parking passes.

ALPR is known by several other names, including Automatic Number Plate Recognition (ANPR), Automatic Vehicle Identification (AVI), Car Plate Recognition (CPR), License Plate Recognition (LPR), and Lecture Automatique de Plaques d'Immatriculation (LAPI).

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7216 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

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

From:	Egnitz, Brian (POL)
To:	Michael Roth
Cc:	John Tedona; Peter Crary
Subject:	RE: DEA Plug-In
Date:	Tuesday, June 27, 2017 12:00:00 PM
Attachments:	image001.png

So the output xml is different than the reads coming in from the cameras? My only issue using the federated search is the hotlist, wouldn't I need to deploy them on both boss servers to get alerts?

From: Michael Roth [mailto:mbroth@mmm.com]
Sent: Tuesday, June 27, 2017 11:49 AM
To: Egnitz, Brian (POL)
Cc: John Tedona; Peter Crary
Subject: RE: DEA Plug-In

Hey Brian, the DEA plugin for Boss is just a file out putter, Boss has no option to import XML data back in from other sources.

Your best bet is the use Boss built in sharing feature, attached is the setup doc, and see section 6 in manual. Port used for sharing is 23032 TCP

3M Science. Applied to Life.™
Michael B. Roth | Application Engineer
3M Traffic Safety Systems Division
3M Center, 235 | St. Paul, MN. 55144
Mobile: +1 513 767 7610
mbroth@mmm.com | www.3M.com
3M ALPR Support Line: 877 777 3571 | alprsupportus@mmm.com

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, June 27, 2017 10:23 AM
To: John Tedona <jtedona@mmm.com>
Cc: Michael Roth <mbroth@mmm.com>
Subject: [EXTERNAL] RE: DEA Plug-In

I read through the documentation and it looks like this plugin could be used to pass info between BOSS systems. Do you know what XML it produces or if BOSS can take the feed like a camera feed. This would be a good solution for us were communities want to locally host BOSS but submit data. Can we get on a call with Peter to discuss?

-Brian

From: John Tedona [mailto:jtedona@mmm.com]
Sent: Friday, June 23, 2017 3:34 PM
To: Egnitz, Brian (POL)
Cc: Michael Roth
Subject: DEA Plug-In

Brian,

If you wanted to check out the DEA Plug-In that I had mentioned to you this morning, the below link is to download the DEA plugin for Boss, instructions are indicated in .Doc file.

https://app.box.com/s/mpxmdewxhheuvxdn2nmuwgj4mfaq7iyk

Steve implantation of plugin is straight forwarded, follow the .doc guide.

General guide:

1. Pick which plugin to use- two are provided. Do not use both only one can be implemented. Typ. used is the one labeled Reads and Hits.
2. Stop Boss server
3. Drop contest of selected plugin into the Boss\plugins folder, located where Boss is installed Typ= "C:\Program Files (x86)\PIPS Technology, Inc\BOSS3\plugins"
4. Edit the BOSS.DEA.plugin.dll.config file.
   a. "MessageDirectroy" = folder path where you want the XML output files to be dropped.
   b. "ORI" = Enter your ORI number.
5. Restart Boss service.
6. Once new reads and or hits come into Boss the XML files will be dropped into folder path indicated from "MessageDirctory".
7. Done

Setting up the DEA file transported instructions is provide by others as we do not have any information regarding this setup.

PS –Kris Wright is out of the office until July 5th, but I asked if someone else from MHQ can send you the P492 price quote in his absence.

Thanks,

3M Science. Applied to Life.™

John Tedona | Public Security | Northeast Sales Manager
TSSD, U.S. Public Security
St. Paul, MN, 3M Center, Bldg. 235-3A-09 | St. Paul, MN 55144-1000
Mobile: 201 841 6237
jtedona@mmm.com | www.3M.com/mvss
3M ALPR Customer Support: alprsupportus@mmm.com | 877-777-3571

3M security scanners have not detected any malicious content in this message.
Click here to report this email as spam

From: Michael Roth
To: Egnitz, Brian (POL)
Cc: John Tedona; Peter Crary
Subject: RE: DEA Plug-In
Date: Tuesday, June 27, 2017 11:51:56 AM
Attachments: image002.png
BOSS 3.0 Inter-agency data sharing How To.docx
BOSS_3.2_User_Manual.pdf

Hey Brian, the DEA plugin for Boss is just a file out putter, Boss has no option to import XML data back in from other sources.

Your best bet is the use Boss built in sharing feature, attached is the setup doc, and see section 6 in manual. Port used for sharing is 23032 TCP

3M Science. Applied to Life.™
Michael B. Roth | Application Engineer
3M Traffic Safety Systems Division
3M Center, 235 | St. Paul, MN. 55144
Mobile: +1 513 767 7610
mbroth@mmm.com | www.3M.com
3M ALPR Support Line: 877 777 3571 | alprsupportus@mmm.com

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, June 27, 2017 10:23 AM
To: John Tedona <jtedona@mmm.com>
Cc: Michael Roth <mbroth@mmm.com>
Subject: [EXTERNAL] RE: DEA Plug-In

I read through the documentation and it looks like this plugin could be used to pass info between BOSS systems. Do you know what XML it produces or if BOSS can take the feed like a camera feed. This would be a good solution for us were communities want to locally host BOSS but submit data. Can we get on a call with Peter to discuss?

-Brian

From: John Tedona [mailto:jtedona@mmm.com]
Sent: Friday, June 23, 2017 3:34 PM
To: Egnitz, Brian (POL)
Cc: Michael Roth
Subject: DEA Plug-In

Brian,

If you wanted to check out the DEA Plug-In that I had mentioned to you this morning, the below link

is to download the DEA plugin for Boss, instructions are indicated in .Doc file.

https://app.box.com/s/mpxmdewxhheuvxdn2nmuwgj4mfaq7iyk

Steve implantation of plugin is straight forwarded, follow the .doc guide.

General guide:

1. Pick which plugin to use- two are provided. Do not use both only one can be implemented. Typ. used is the one labeled Reads and Hits.
2. Stop Boss server
3. Drop contest of selected plugin into the Boss\plugins folder, located where Boss is installed Typ= "C:\Program Files (x86)\PIPS Technology, Inc\BOSS3\plugins"
4. Edit the BOSS.DEA.plugin.dll.config file.
    a. "MessageDirectroy" = folder path where you want the XML output files to be dropped.
    b. "ORI" = Enter your ORI number.
5. Restart Boss service.
6. Once new reads and or hits come into Boss the XML files will be dropped into folder path indicated from "MessageDirctory".
7. Done

Setting up the DEA file transported instructions is provide by others as we do not have any information regarding this setup.

PS –Kris Wright is out of the office until July 5th, but I asked if someone else from MHQ can send you the P492 price quote in his absence.

Thanks,

3M Science. Applied to Life.™

John Tedona | Public Security | Northeast Sales Manager
TSSD, U.S. Public Security
St. Paul, MN, 3M Center, Bldg. 235-3A-09 | St. Paul, MN 55144-1000
Mobile: 201 841 6237
jtedona@mmm.com | www.3M.com/mvss
3M ALPR Customer Support: alprsupportus@mmm.com | 877-777-3571

3M security scanners have not detected any malicious content in this message.
Click here to report this email as spam

From: Michael Roth
To: Egnitz, Brian (POL)
Cc: John Tedona; Peter Crary
Subject: RE: DEA Plug-In
Date: Tuesday, June 27, 2017 2:53:56 PM
Attachments: image001.png

Correct XML output is different than the way Boss can accept reads coming in.

With Boss, Sharing. two ways to get notified that I can see.

1. Boss has a "remote alerts to" setting in hotlist section where you would select you remote site to get alerts, though I'm not 100% of how this behaver works as the manual indicates alerts from this holtlist would come into remote system as read- so to your point you may have to deploy similar alert list.
2. Since you'll already be setting up remote search access on other systems you could just as easily add email notifications to the alerts.

3M Science. Applied to Life.™

Michael B. Roth | Application Engineer
3M Traffic Safety Systems Division
3M Center, 235 | St. Paul, MN. 55144
Mobile: +1 513 767 7610
mbroth@mmm.com | www.3M.com
3M ALPR Support Line: 877 777 3571 | alprsupportus@mmm.com

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, June 27, 2017 12:01 PM
To: Michael Roth <mbroth@mmm.com>
Cc: John Tedona <jtedona@mmm.com>; Peter Crary <pcrary@mmm.com>
Subject: [EXTERNAL] RE: DEA Plug-In

So the output xml is different than the reads coming in from the cameras? My only issue using the federated search is the hotlist, wouldn't I need to deploy them on both boss servers to get alerts?

From: Michael Roth [mailto:mbroth@mmm.com]
Sent: Tuesday, June 27, 2017 11:49 AM
To: Egnitz, Brian (POL)
Cc: John Tedona; Peter Crary
Subject: RE: DEA Plug-In

Hey Brian, the DEA plugin for Boss is just a file out putter, Boss has no option to import XML data back in from other sources.

Your best bet is the use Boss built in sharing feature, attached is the setup doc, and see section 6 in manual. Port used for sharing is 23032 TCP

3M Science. Applied to Life.™
Michael B. Roth | Application Engineer
3M Traffic Safety Systems Division
3M Center, 235 | St. Paul, MN. 55144
Mobile: +1 513 767 7610
mbroth@mmm.com | www.3M.com
3M ALPR Support Line: 877 777 3571 | alprsupportus@mmm.com

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, June 27, 2017 10:23 AM
To: John Tedona <jtedona@mmm.com>
Cc: Michael Roth <mbroth@mmm.com>
Subject: [EXTERNAL] RE: DEA Plug-In

I read through the documentation and it looks like this plugin could be used to pass info between BOSS systems. Do you know what XML it produces or if BOSS can take the feed like a camera feed. This would be a good solution for us were communities want to locally host BOSS but submit data. Can we get on a call with Peter to discuss?

-Brian

From: John Tedona [mailto:jtedona@mmm.com]
Sent: Friday, June 23, 2017 3:34 PM
To: Egnitz, Brian (POL)
Cc: Michael Roth
Subject: DEA Plug-In

Brian,

If you wanted to check out the DEA Plug-In that I had mentioned to you this morning, the below link is to download the DEA plugin for Boss, instructions are indicated in .Doc file.

https://app.box.com/s/mpxmdewxhheuvxdn2nmuwgj4mfaq7iyk

Steve implantation of plugin is straight forwarded, follow the .doc guide.

General guide:

1. Pick which plugin to use- two are provided. Do not use both only one can be implemented.

Typ. used is the one labeled Reads and Hits.

2. Stop Boss server
3. Drop contest of selected plugin into the Boss\plugins folder, located where Boss is installed Typ= "C:\Program Files (x86)\PIPS Technology, Inc\BOSS3\plugins"
4. Edit the BOSS.DEA.plugin.dll.config file.
   a. "MessageDirectroy" = folder path where you want the XML output files to be dropped.
   b. "ORI" = Enter your ORI number.
5. Restart Boss service.
6. Once new reads and or hits come into Boss the XML files will be dropped into folder path indicated from "MessageDirctory".
7. Done

Setting up the DEA file transported instructions is provide by others as we do not have any information regarding this setup.

PS –Kris Wright is out of the office until July 5th, but I asked if someone else from MHQ can send you the P492 price quote in his absence.

Thanks,

3M Science. Applied to Life.™

John Tedona | Public Security | Northeast Sales Manager
TSSD, U.S. Public Security
St. Paul, MN, 3M Center, Bldg. 235-3A-09 | St. Paul, MN 55144-1000
Mobile: 201 841 6237
jtedona@mmm.com | www.3M.com/mvss
3M ALPR Customer Support: alprsupportus@mmm.com | 877-777-3571

3M security scanners have not detected any malicious content in this message.
Click here to report this email as spam

3M security scanners have not detected any malicious content in this message.
Click here to report this email as spam

From: John Tedona CW
To: Egnitz, Brian (POL); Hughes, Sean (EPS)
Cc: Quinn, Dermot (POL); Mason, Christopher (POL); Noonan, David (POL); pcrary@neology.net
Subject: RE: LPR Stats for storage
Date: Friday, September 8, 2017 4:12:31 PM

Brian,

For Mobile Systems use 70KB per read rather than 200KB.

200KB per read for a fixed camera is fine.

3M Science. Applied to Life.™

John Tedona | Public Security | Northeast Sales Manager
TSSD, U.S. Public Security
St. Paul, MN, 3M Center, Bldg. 235-3A-09 | St. Paul, MN 55144-1000
Mobile: 201 841 6237
jtedona@mmm.com | www.3M.com/mvss
3M ALPR Customer Support: alprsupportus@mmm.com | 877-777-3571

From: Egnitz, Brian (POL) [mailto:brian.egnitz@MassMail.State.MA.US]
Sent: Thursday, September 07, 2017 4:42 PM
To: Hughes, Sean (EPS) <sean.hughes@state.ma.us>
Cc: Quinn, Dermot (POL) <dermot.quinn@state.ma.us>; Mason, Christopher (POL) <chris.mason@state.ma.us>; Noonan, David (POL) <dnoonan@massport.com>; John Tedona CW <jtedona@mmm.com>; pcrary@neology.net
Subject: [EXTERNAL] LPR Stats for storage

Hi Sean,

Per our conversation, here are some storage estimates. I'll know more in 2 weeks whether Neology can provide a BOSS plug-in to support data transfer from Boston and Massport to the central BOSS server at Chelsea. I've included some of the Neology team on the thread to check my math.

Current Plate Count: **135,407,037**
Current storage **13.9 TB** with **1.4T** available
Estimated that there are currently 70 Cameras currently contributing, 25 Fixed with 45 Mobile
Oldest record is "2015-06-12 18:21:29.143" **** not sure what this isn't being purged***
We **would need an additional 12 TB** to be added to allow new MSP cameras, BPD existing cameras and MassPort Cameras to retain for 1 year (this can be done in batches, the Boston sharing agreement isn't done yet and MassPort will be rolling cameras out slowly)

Worst case storage scenario:

Mobile Camera

- 1 Mobile Camera @ 8,000 Max reads per day @ 200 KB per read = 1.5258 GB per camera per day (556.917 GB per year)
- 45 Mobile Cameras = 68 GB per day
- @365 = 24,616 GB or 24 TB per year

Fixed Cameras

- 1 Fixed Camera @ 15,000 Max reads per day @ 200 KB per read = 2.861 GB per camera per day (1,044.265 GB per year)
- 25 Fixed Cameras = 71 GB per day
- @365 = 26,106 GB or 25 TB per year

With these calculations our storage should be 49 TB.
Each new fixed camera would require 1 TB and each new mobile camera would require .5 TB to be added to retain for one year.

If we adjust by 3.5 (our current storage / estimated)
Each Fixed = 298 GB per year
Each Mobile = 159 GB per year

MSP will be adding 9 new LPRS and will need 2.6 TB
Massport 25 fixed would need 7.2 TB
BPD 8 fixed would need 2.3 TB

Action Items:

We need to figure out why the purge isn't working
We need to find out if Neology can push a copy of the data from the other BOSS systems
We would evaluate the architecture (need to evaluate the app server for performance, we should look at backups, DB clustering for redundancy and maintenance alerts)
Firewalls would need to be opened to allow both federated search and submittal of reads

- Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7216 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

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

3M security scanners have not detected any malicious content in this message.
Click here to report this email as spam

From: Farrell, Sean (POL)
To: Halpin, Michael (POL)
Subject: RE: MOU Re: ALPR on MassDOT Property
Date: Wednesday, April 5, 2017 5:21:00 PM
Attachments: ALPR Agreement 24925.docx

Mike – the MOU has an indemnification clause in it. Also, there's a public records responsibility clause there as well. See highlights. Sean

---

From: Halpin, Michael (POL)
Sent: Tuesday, April 04, 2017 5:20 PM
To: Hiitt, Katelyn (POL)
Cc: Farrell, Sean (POL)
Subject: FW: MOU Re: ALPR on MassDOT Property

Sean: Please review and see me to discuss. Thanks.

From: Fenton, Eileen (DOT) [mailto:eileen.fenton@dot.state.ma.us]
Sent: Tuesday, April 04, 2017 4:18 PM
To: Amodeo, Edward (POL); Quinn, Dermot (POL); Halpin, Michael (POL); Hanson, Terry (POL)
Subject: FW: MOU Re: ALPR on MassDOT Property

Good Afternoon,
Attached for your review and comment is a draft of the MOU between MassDOT and the State Police for installation of ALPR equipment on MassDOT property. As discussed, the agreement is not site specific. In the event you are interested in a specific location, the agreement provides that you will submit the plans to MassDOT for review and approval, as appropriate.

Once I receive your comments, I will send along to Tom Tinlin for review.

Please let me know if you have any questions.

Thank you.
Eileen

Eileen M. Fenton
Senior Counsel
Massachusetts Department of Transportation
Ten Park Plaza, Suite 3510
Boston, Massachusetts 02116
T: 857-368-8764
Eileen.Fenton@state.ma.us

From: Farrell, Sean (POL)
To: Halpin, Michael (POL)
Subject: RE: MOU Re: ALPR on MassDOT Property
Date: Wednesday, April 5, 2017 5:21:00 PM
Attachments: ALPR Agreement 24925.docx

Mike – the MOU has an indemnification clause in it. Also, there's a public records responsibility clause there as well. See highlights. Sean

---

From: Halpin, Michael (POL)
Sent: Tuesday, April 04, 2017 5:20 PM
To: Hiitt, Katelyn (POL)
Cc: Farrell, Sean (POL)
Subject: FW: MOU Re: ALPR on MassDOT Property

Sean: Please review and see me to discuss. Thanks.

From: Fenton, Eileen (DOT) [mailto:eileen.fenton@dot.state.ma.us]
Sent: Tuesday, April 04, 2017 4:18 PM
To: Amodeo, Edward (POL); Quinn, Dermot (POL); Halpin, Michael (POL); Hanson, Terry (POL)
Subject: FW: MOU Re: ALPR on MassDOT Property

Good Afternoon,
Attached for your review and comment is a draft of the MOU between MassDOT and the State Police for installation of ALPR equipment on MassDOT property. As discussed, the agreement is not site specific. In the event you are interested in a specific location, the agreement provides that you will submit the plans to MassDOT for review and approval, as appropriate.

Once I receive your comments, I will send along to Tom Tinlin for review.

Please let me know if you have any questions.

Thank you.
Eileen

Eileen M. Fenton
Senior Counsel
Massachusetts Department of Transportation
Ten Park Plaza, Suite 3510
Boston, Massachusetts 02116
T: 857-368-8764
Eileen.Fenton@state.ma.us

From: John Tedona CW
To: Egnitz, Brian (POL)
Subject: RE: Nutanix / Public Sector - Meeting Request
Date: Tuesday, July 11, 2017 12:53:17 PM

Nutanix is not us. I'm now Neology Inc.

The sales was completed on July 1st, but during the transition process I still have access the 3M email and my phone number will remain unchanged. Below is an email that I had sent to my dealers such as MHQ. I'll be at 3M HQ in St. Paul MN this week for another transition meeting.

_____

It's official -3M has completed the previously announced sale of its tolling and automated license/number plate recognition (ALPR) business to Neology, Inc., a leading provider of integrated solutions for tolling, electronic vehicle registration and public safety applications.

To help facilitate a smooth transfer of operations and minimize disruption, for a limited time, 3M will provide certain transition services in connection with this business.

Ordering
During this transition period, you will continue to interface with 3M as before for ordering, shipping and invoicing of all tolling and ALPR products.

Important Note Regarding Invoice Payment
Please note that you should pay all invoices to the remit address on that specific invoice. During the upcoming transition, invoices with a 3M remit address are payable directly to 3M.

Please click the link below to read the Neology press release announcement...
http://www.globenewswire.com/news-release/2017/06/30/1035610/0/en/Neology-Completes-Acquisition-of-3M-s-Tolling-and-License-Plate-Recognition-Business.html

3M Science. Applied to Life.™

John Tedona | Public Security | Northeast Sales Manager
TSSD, U.S. Public Security
St. Paul, MN, 3M Center, Bldg. 235-3A-09 | St. Paul, MN 55144-1000
Mobile: 201 841 6237
jtedona@mmm.com | www.3M.com/mvss
3M ALPR Customer Support: alprsupportus@mmm.com | 877-777-3571

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, July 11, 2017 12:42 PM
To: John Tedona CW <jtedona@mmm.com>
Subject: [EXTERNAL] Fwd: Nutanix / Public Sector - Meeting Request

Is this the new company that owns you guys now?

Begin forwarded message:

From: Trey Helms <trey.helms@nutanix.com>
Date: July 11, 2017 at 9:14:11 AM PDT
To: brian.egnitz@massmail.state.ma.us
Subject: Nutanix / Public Sector - Meeting Request

Hi Brian,

I am part of the public sector support team here at Nutanix, and I was asked to reach out to you personally to connect with us for an educational call with our team. I'm not sure how familiar you are with Nutanix or our impact within the public sector so I built out a few bullet points you can flip through before our first sync up.

- Nutanix has enterprise deployments in many large communities and universities, to name a few:
    1. Boston University
    2. Several state Departments within NY, NJ, NC, MD
    3. New York University
- Nutanix also maintains deployments in several small cities and counties
- Nutanix is the ONLY DoD STIG'ed system out of the box (with RMF compliance)
- Nutanix is the ONLY vendor who supports multi-hypervisor with tools to convert between them
- If your budget is decreasing and requirements are increasing, we can share with you examples of how we have helped other Civilian and DOD customers address these challenges.

Below are some of the questions and concerns we typically address on first calls/educational. If any of these apply please highlight so we can discuss on our call, or if you would like to speak offline feel free to give me a call. We can walk through a Nutanix 101, discuss use cases and references if you do not have any specific needs or questions.

1. Is data space and power an issue?
2. Any remote or branch office requirements
3. Issues with complexity or STIG / audits?
4. Walk me through current process to upgrade SAN/ server when an IAVA comes out…how long does it take to create an artifact for IA?
5. Any new virtual workloads?

Lastly, do you have an hour in the next 1-2 weeks to jump on a webex with one of our account teams? I will send out a calendar invite with webex info once we get a good time to hard slot.

Thank you and we look forward to speaking with you and your team shortly.

--
Trey Helms
Sales Development Representative | Nutanix
(919) 724-4257



3M security scanners have not detected any malicious content in this message.
Click here to report this email as spam

From: Thibault, Amy (POL)
To: Pinkes, William (POL)
Cc: Mason, Christopher (POL)
Subject: RE: SPEAR Training
Date: Friday, October 6, 2017 2:22:00 PM
Attachments: Databases.xlsx
image001.png
image002.png

Capt. Pinkes,

I have updated the attached spreadsheet with the data I am aware of and have added a few additional trainings they should receive. Please let me know if you have questions or need anything else.

Respectfully,

Amy

From: Pinkes, William (POL)
Sent: Tuesday, October 03, 2017 11:11 AM
To: Thibault, Amy (POL)
Cc: Mason, Christopher (POL)
Subject: SPEAR Training

Good morning Amy,

I am trying to identify the training we will need to provide our analysts. I would like to set up a training itinerary to allow us to schedule the appropriate amount of time and identify the instructors we will need to have on board.

If you have a moment to review the below list, could you help me identify the instructors and, if known, the amount of training time necessary. If you are unsure of the time necessary to train I will contact the instructor(s) directly.

I will address the CJIS related training components.

While many of the workers are contract workers that are in need of only a refresher I would prefer to train all 6 to the same standard, the 3 contract workers can sit side by side with a new worker during the training and provide assistance which will also help with team building. I anticipate we will provide this training at the SPEAR unless necessity requires it be held in Maynard.

Thank you for your help with this request.

Captain William M. Pinkes
Communications Section
470 Worcester Road
Framingham, MA 01702
508-988-7060

From: Ghasemi, Kiarash (POL)
Sent: Friday, September 29, 2017 2:29 PM
To: Pinkes, William (POL) <William.Pinkes@MassMail.State.MA.US>
Cc: Hernandez, Oscar (POL) <Oscar.Hernandez@MassMail.State.MA.US>; Weldon, Stephen (POL) <Stephen.Weldon@MassMail.State.MA.US>
Subject: RE: Updated Application List

Hi Capt.

Bellow please find status of the SPEAR Check list

Application	Status	Administrator
CopLink	Done	CFC
CrimeNtel	Done	CFC
ACISS	Done	CFC
ISO	Done	
L-1 Facial Rec	Done	None
Issuance 360 Facial Rec	Done	None
Boss 3M LPR	Done	Lt. Dan Griffin
Vigilant LPR	Done	Shannan Clark
CJIS	Done	None
Extranet	Done	None
Inmate Web	Done	None
Clear	Done	
Fox Messenger	Done	DCJIS
Adobe Acrobat Pro	**Pending Approval**	
RAMS	Done	MIS
MS Office	**Pending Approval**	
Twitter	Done	None
Tweet Deck	Done	None
Facebook	Done	None
Instagram	Done	None

Snapchat	Done	None
Photoshop	Done	
Sharepoint	Done	CFC
Open Source Intel Tecniques	Done	NA
HHAN	Done	CFC
HSIN	Done	DHS
National Situation Awareness Room	**Pending More Info**	DHS
Downlink	Done	DAS
Analyst Notebook	**Pending More Info**	
FinCEN	Done	
Spear email	**Pending Approval**	
AM Reports	Done	
HSDN	Done	

From: Pinkes, William (POL)
Sent: Friday, September 29, 2017 10:15 AM
To: Ghasemi, Kiarash (POL)
Subject: FW: Updated Application List

FYI, on my way down to SPEAR now.

Captain William M. Pinkes
Communications Section
470 Worcester Road
Framingham, MA 01702
508-988-7060

From: Commonwealth Fusion Center (POL)
Sent: Friday, September 29, 2017 9:48 AM
To: Pinkes, William (POL) <William.Pinkes@MassMail.State.MA.US>
Cc: Archive Fusion <fusionarchive@disnet.pol.state.ma.us>
Subject: Updated Application List

Captain,

Updated the list to fill in some of the blanks. I do not have access to the HSIN Situational Awareness Room, so I'll have to talk to Shannan on Monday to get the direct link, but I suspect it can be

accessed through the main HSIN page as well. For the Boss 3M ALPR application, our shortcuts are routed from our CIS shared (M:/) drive under the SA Client 3.2.0 folder which contains a .exe for the client:

\\msp-fp-cis\cis_per\SA Client 3.2.0
Then run the executable

Respectfully,

Sean Bender
Massachusetts State Police
Commonwealth Fusion Center
124 Acton Street
Maynard, MA 01754
978-451-3700 (phone)
978-451-3707 (fax)

From: Thibault, Amy (POL)
To: Pinkes, William (POL)
Cc: Mason, Christopher (POL)
Subject: RE: SPEAR Training
Date: Friday, October 6, 2017 2:22:50 PM
Attachments: Databases.xlsx
image001.png
image002.png

Capt. Pinkes,

I have updated the attached spreadsheet with the data I am aware of and have added a few additional trainings they should receive. Please let me know if you have questions or need anything else.

Respectfully,

Amy

From: Pinkes, William (POL)
Sent: Tuesday, October 03, 2017 11:11 AM
To: Thibault, Amy (POL)
Cc: Mason, Christopher (POL)
Subject: SPEAR Training

Good morning Amy,

I am trying to identify the training we will need to provide our analysts. I would like to set up a training itinerary to allow us to schedule the appropriate amount of time and identify the instructors we will need to have on board.

If you have a moment to review the below list, could you help me identify the instructors and, if known, the amount of training time necessary. If you are unsure of the time necessary to train I will contact the instructor(s) directly.

I will address the CJIS related training components.

While many of the workers are contract workers that are in need of only a refresher I would prefer to train all 6 to the same standard, the 3 contract workers can sit side by side with a new worker during the training and provide assistance which will also help with team building. I anticipate we will provide this training at the SPEAR unless necessity requires it be held in Maynard.

Thank you for your help with this request.

Captain William M. Pinkes
Communications Section
470 Worcester Road
Framingham, MA 01702
508-988-7060

From: Ghasemi, Kiarash (POL)
Sent: Friday, September 29, 2017 2:29 PM
To: Pinkes, William (POL) <William.Pinkes@MassMail.State.MA.US>
Cc: Hernandez, Oscar (POL) <Oscar.Hernandez@MassMail.State.MA.US>; Weldon, Stephen (POL) <Stephen.Weldon@MassMail.State.MA.US>
Subject: RE: Updated Application List

Hi Capt.

Bellow please find status of the SPEAR Check list

Application	Status	Administrator
CopLink	Done	CFC
CrimeNtel	Done	CFC
ACISS	Done	CFC
ISO	Done	
L-1 Facial Rec	Done	None
Issuance 360 Facial Rec	Done	None
Boss 3M LPR	Done	Lt. Dan Griffin
Vigilant LPR	Done	Shannan Clark
CJIS	Done	None
Extranet	Done	None
Inmate Web	Done	None
Clear	Done	
Fox Messenger	Done	DCJIS
Adobe Acrobat Pro	**Pending Approval**	
RAMS	Done	MIS
MS Office	**Pending Approval**	
Twitter	Done	None
Tweet Deck	Done	None
Facebook	Done	None
Instagram	Done	None

Snapchat	Done	None
Photoshop	Done	
Sharepoint	Done	CFC
Open Source Intel Tecniques	Done	NA
HHAN	Done	CFC
HSIN	Done	DHS
National Situation Awareness Room	**Pending More Info**	DHS
Downlink	Done	DAS
Analyst Notebook	**Pending More Info**	
FinCEN	Done	
Spear email	**Pending Approval**	
AM Reports	Done	
HSDN	Done	

From: Pinkes, William (POL)
Sent: Friday, September 29, 2017 10:15 AM
To: Ghasemi, Kiarash (POL)
Subject: FW: Updated Application List

FYI, on my way down to SPEAR now.

Captain William M. Pinkes
Communications Section
470 Worcester Road
Framingham, MA 01702
508-988-7060

From: Commonwealth Fusion Center (POL)
Sent: Friday, September 29, 2017 9:48 AM
To: Pinkes, William (POL) <William.Pinkes@MassMail.State.MA.US>
Cc: Archive Fusion <fusionarchive@disnet.pol.state.ma.us>
Subject: Updated Application List

Captain,

Updated the list to fill in some of the blanks. I do not have access to the HSIN Situational Awareness Room, so I'll have to talk to Shannan on Monday to get the direct link, but I suspect it can be

accessed through the main HSIN page as well. For the Boss 3M ALPR application, our shortcuts are routed from our CIS shared (M:/) drive under the SA Client 3.2.0 folder which contains a .exe for the client:

\\msp-fp-cis\cis_per\SA Client 3.2.0
Then run the executable

Respectfully,

Sean Bender
Massachusetts State Police
Commonwealth Fusion Center
124 Acton Street
Maynard, MA 01754
978-451-3700 (phone)
978-451-3707 (fax)

From: Griffin, Daniel (POL)
To: Larason, Jeff (OGR)
Subject: Re: TSRP - LE Partnership - CARS
Date: Wednesday, February 1, 2017 1:01:10 PM
Attachments: TSRP%20MSP%20%20proposal1.doc

Jeff-
Here it is, however, this time I am sending you the CORRECT version (my apologies, not sure how that happened). I'll be back in on
Tuesday if you have any questions.
Thanks
Dan

Lieutenant Daniel J. Griffin 1129
Traffic Programs Section
Massachusetts State Police
General Headquarters
470 Worcester Road
Framingham, Ma. 01701

From: Larason, Jeff (OGR)
Sent: Tuesday, January 31, 2017 9:02 AM
To: Griffin, Daniel (POL)
Subject: RE: TSRP - LE Partnership - CARS

Hi Dan,

Thanks. No rush on it. I will start working on it on this end with the draft/cost analysis you sent.

However the draft does not make specific mention of the recent passage of recreational marijuana, which is, I think an important element to include in the Executive Summary and the Statement of Need. If you can make that update it would strengthen the reasoning.

Enjoy OKC. Great town.

Jeff

From: Griffin, Daniel (POL)
Sent: Tuesday, January 31, 2017 8:48 AM
To: Larason, Jeff (OGR)
Subject: Re: TSRP - LE Partnership - CARS

Jeff
I am in OKC. The proposal
I sent you was updated. Will
Attempt to locate remotely. and resend. I
Won't be there Friday. Day off and not allowed to work and bank the day. Sorry Dan

On Jan 31, 2017, at 7:32 AM, Larason, Jeff (OGR) <jeff.larason@MassMail.State.MA.US> wrote:

Hi Dan,

Can you update the TSPR proposal so that it has current language and removes the DRAFT watermark. I'd like to start the process, getting everyone on board, and see if we can make this happen sooner, rather than later.

I'm sorry we missed you yesterday. We had a smaller group attending the forum but had a good discussion none-the-less. We have a good size list of attendees on Friday in Lynn, if you are available to join us.

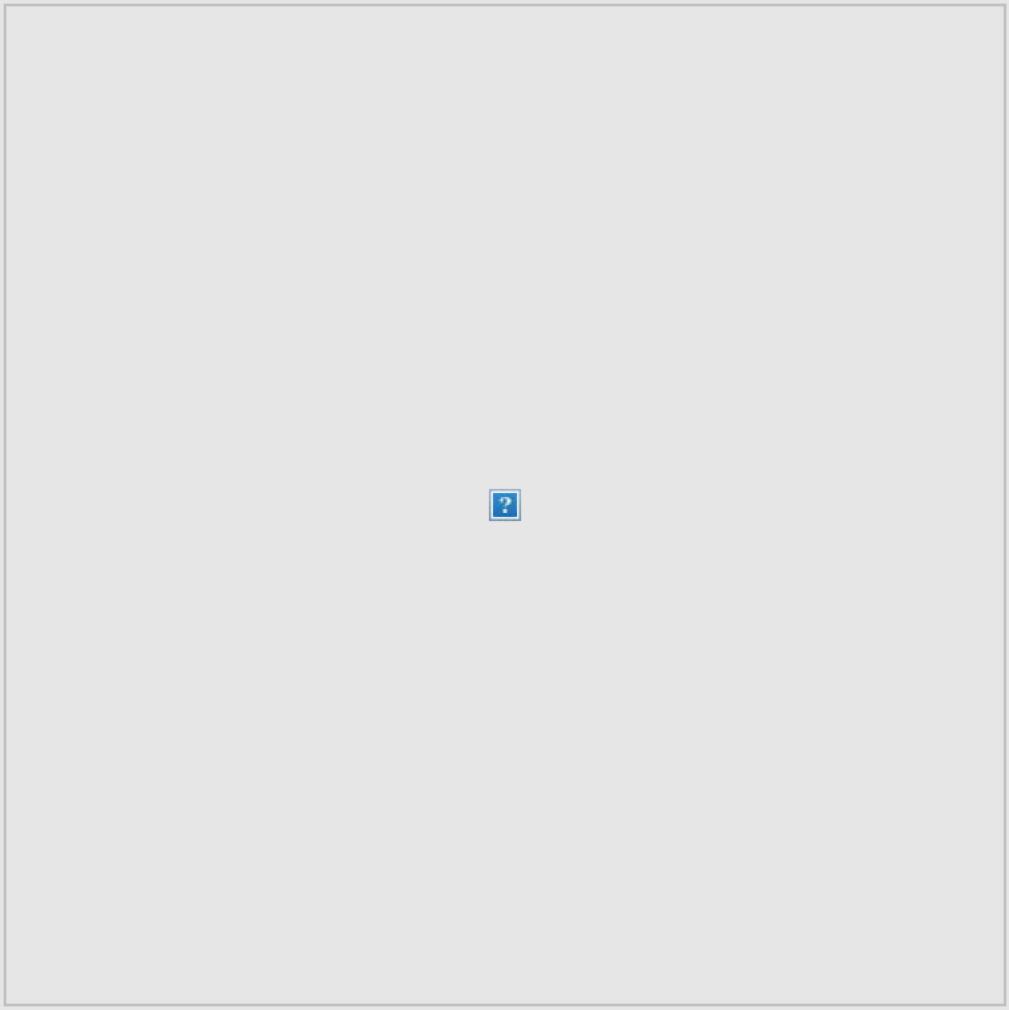
Was there a CARS report from last week?

Jeff

Jeff Larason
Director
Highway Safety Division
Executive Office of Public Safety and Security
Office of Grants and Research
Ten Park Plaza, Suite 3720
Boston, MA 02116
jeff.larason@State.MA.US
617-725-3308
<image007.png><image008.png><image009.jpg>
#CrashNotAccident

From: Traffic Technology Today
To: Dowd, Timothy (POL)
Subject: Toyota invests in MaaS Global
Date: Friday, June 30, 2017 7:30:41 AM

If you are having trouble viewing this email, click here to display it in your web browser



NEW VIDEO: Caltrans installs HAWK pedestrian crosswalk signal

The California Department of Transportation (Caltrans) has installed a new 'high intensity activated crosswalk' (HAWK) beacon at a busy intersection on State Route 108 more...

OPINION: What it means to be an engineer

Michelle Doolan, a civil engineer at Aurecon, argues that engineering is far more than a job. Engineers are the shapers and problem solvers of our collective future. It's about seeing the world at it is and believing we can improve upon it more...

Weekly poll

This week the University of Connecticut's interactive, publicly-available crash database has been receiving national interest (read our full report here). Now we want to know what you think…

Although sharing data is useful, is it necessary for sensitive information, such as details of crashes, to be made available to the public?

- **Yes**
- **No**

Click here to vote now!

Poll results

Last week, Dubai's Road and Transport Authority (RTA) announced its plans to color pavement asphalt to alert drivers of changes in speed limits (read our full report here). We then asked you…

Will the procedure be effective and should road authorities in other countries follow suit? You answered…

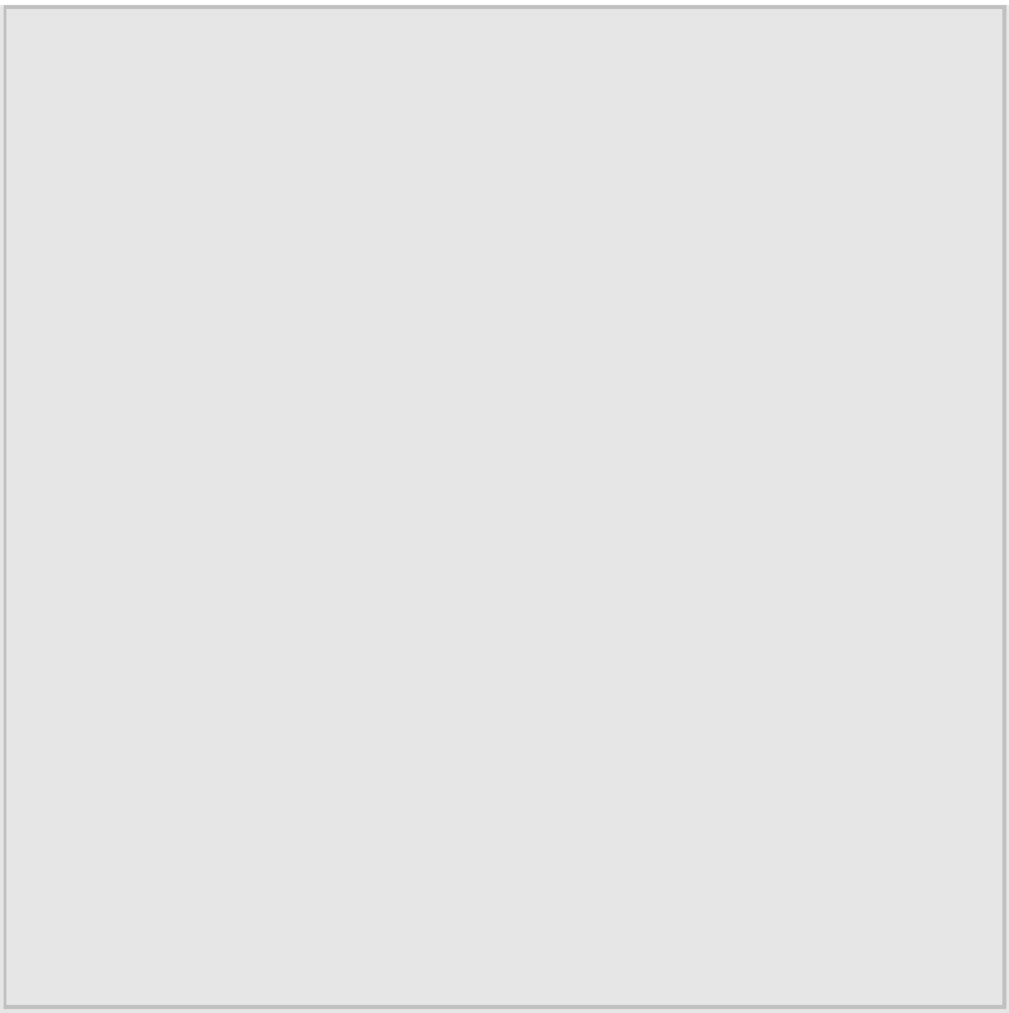
In the news this week

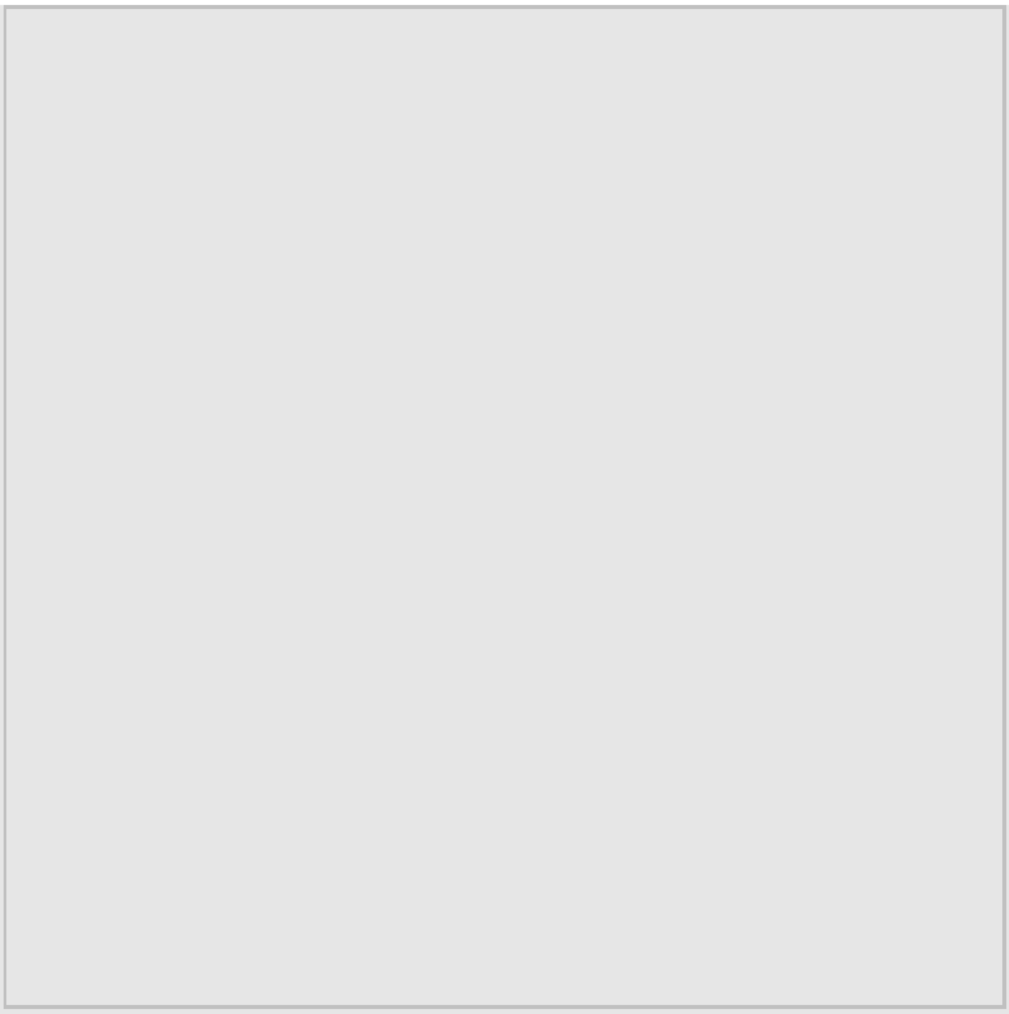
Toyota and its insurance partner make significant investment in MaaS Global

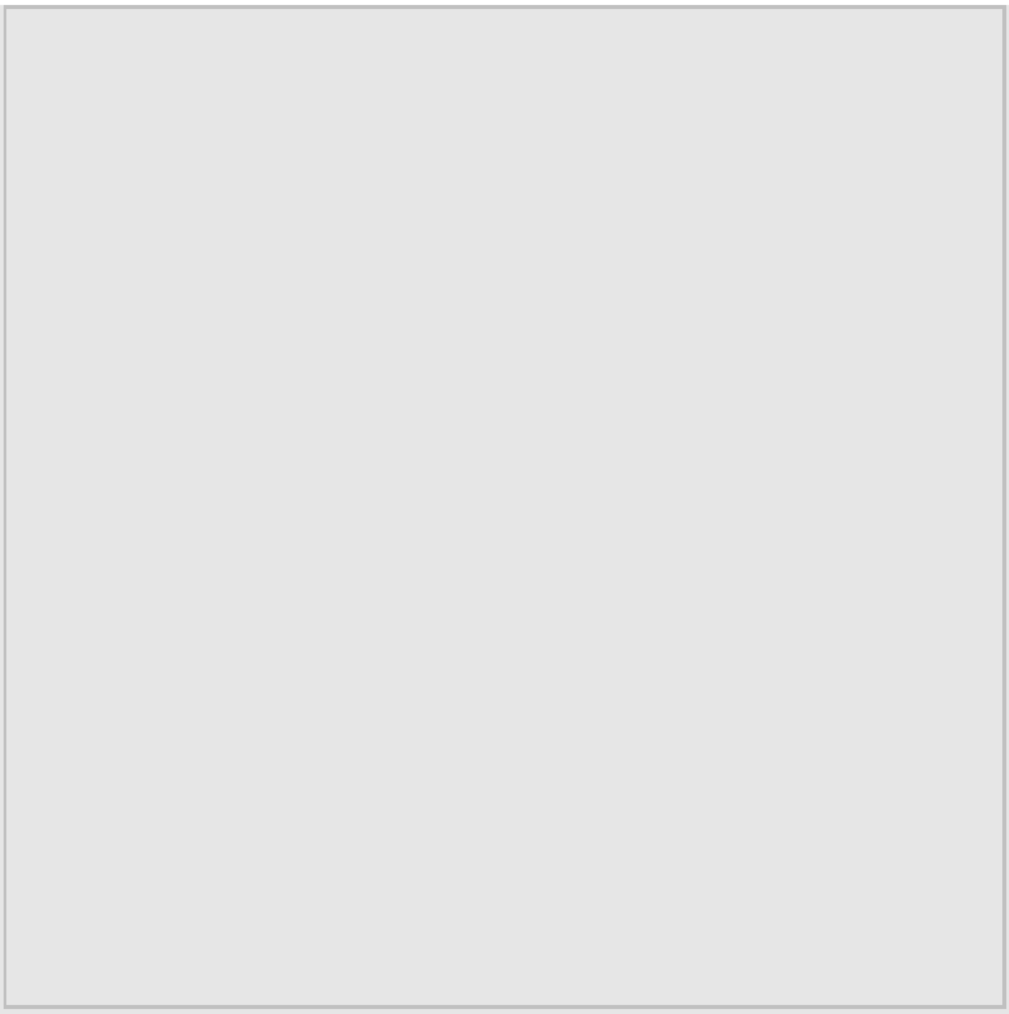
Toyota Financial Services of Japan and its insurance partner, Aioi Nissay Dowa Insurance Company, have become one of the most significant investors in the Finnish company MaaS Global, the leading developer of the Mobility-as-a-Service (MaaS) concept more...

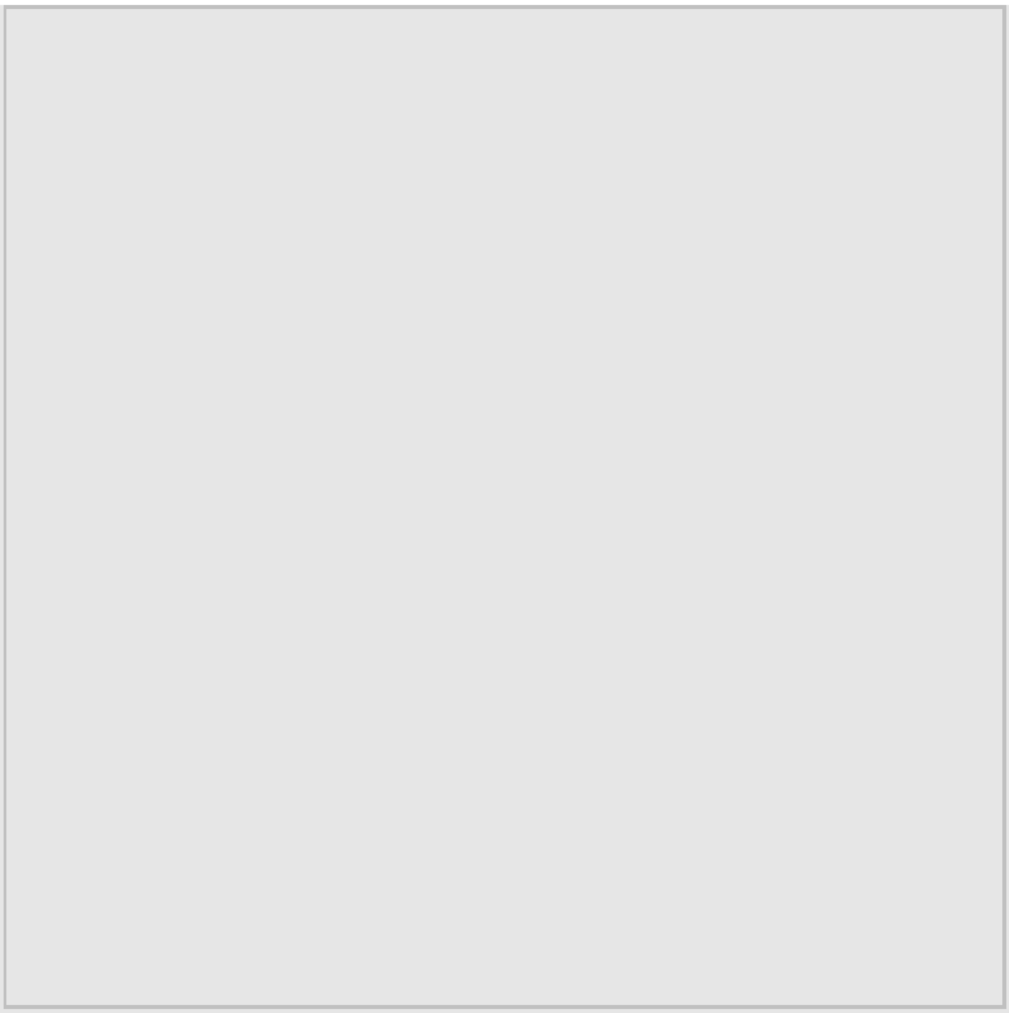
More news...

- European Commission proposes US$3bn investment for 152 transport projects
- USDOT provides US$99.6m loan for multimodal transport project in Washington State
- Road and automotive groups to advance deployment of C-ITS in Europe by 2019
- European Commission presents five Excellence in Road Safety Awards
- System uses streetlights to provide accurate, low-cost traffic counts
- Three consultancies form JV to accelerate California's I-405 Improvement Project
- Jacobs to design active traffic management system for I-76 corridor in Pennsylvania
- Moovit launches mobility data and analytics tools to improve urban transport management
- Minnesota ready to test use of autonomous buses in cold climate conditions
- NEW JOB VANCACIES: Your next career move could be here!









Inside this issue...



<< COVER STORY

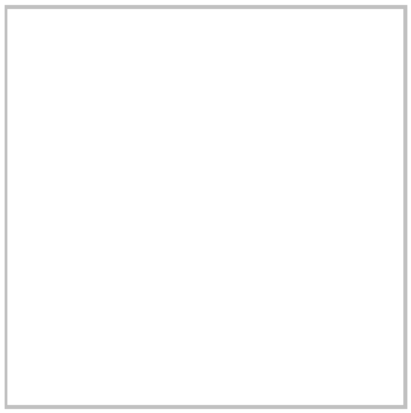
WATCHERS AT THE WALL

What is the best way to protect your borders while processing vehicles at speed? Saul Wordsworth examines a case in point at a border crossing between the USA and Mexico, in Arizona

<< LOW EMISSION ZONES

BREATHE AGAIN

As low emission zones hit headlines across Europe, Jack Roper investigates the challenges involved in using ALPR cameras to enforce such schemes



<< INTERVIEW

JIM O'SULLIVAN

Jim O'Sullivan has enjoyed two successful years as CEO of Highways England. Now he's making plans for even greater achievements in the near future.

This email (which includes any files transmitted with it) is confidential and may also be legally privileged. It is intended solely for the use of the individual to whom it is addressed. Any views or opinions presented are solely those of the author and do not necessarily represent those of UKi Media & Events. If you are not the intended recipient, be advised that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited. If you have received this message in error, do not open any attachment but please notify the sender (above) deleting this message from your system. Please rely on your own anti-virus system, no responsibility is taken by the sender for any damage rising out of virus infection.

UKi Media & Events, a division of UKIP Media & Events Limited
Registered Address: 26 Red Lion Square, London, WC1R 4AG
VAT No. GB879 4451 71
Registration Number: 5893940
Company registered in England and Wales

From: Traffic Technology Today
To: Dowd, Timothy (POL)
Subject: Toyota invests in MaaS Global
Date: Friday, June 30, 2017 7:31:46 AM

If you are having trouble viewing this email, click here to display it in your web browser

NEW VIDEO: Caltrans installs HAWK pedestrian crosswalk signal

The California Department of Transportation (Caltrans) has installed a new 'high intensity activated crosswalk' (HAWK) beacon at a busy intersection on State Route 108 more...

OPINION: What it means to be an engineer

Michelle Doolan, a civil engineer at Aurecon, argues that engineering is far more than a job. Engineers are the shapers and problem solvers of our collective future. It's about seeing the world at it is and believing we can improve upon it more...

Weekly poll

This week the University of Connecticut's interactive, publicly-available crash database has been receiving national interest (read our full report here). Now we want to know what you think…

Although sharing data is useful, is it necessary for sensitive information, such as details of crashes, to be made available to the public?

- **Yes**
- **No**

Click here to vote now!

Poll results

Last week, Dubai's Road and Transport Authority (RTA) announced its plans to color pavement asphalt to alert drivers of changes in speed limits (read our full report here). We then asked you…

Will the procedure be effective and should road authorities in other countries follow suit? You answered…

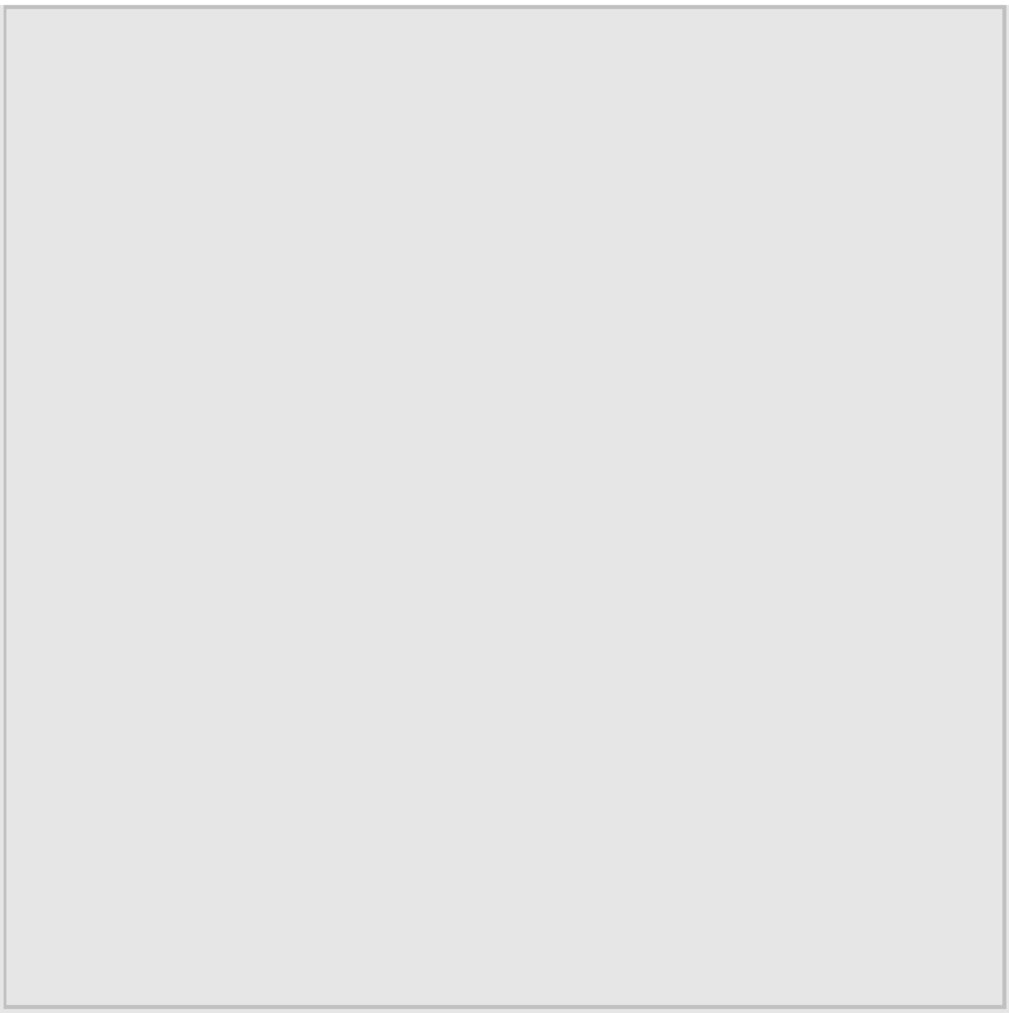
In the news this week

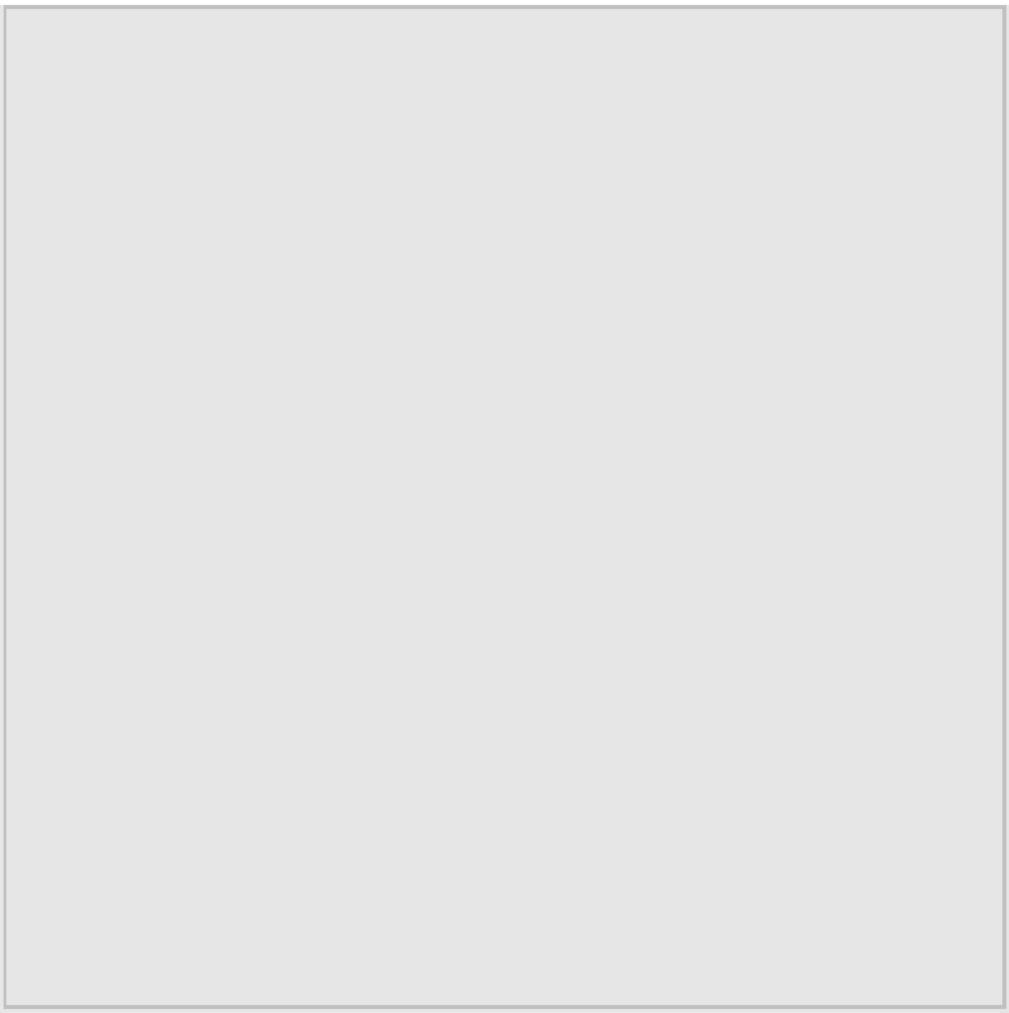
Toyota and its insurance partner make significant investment in MaaS Global

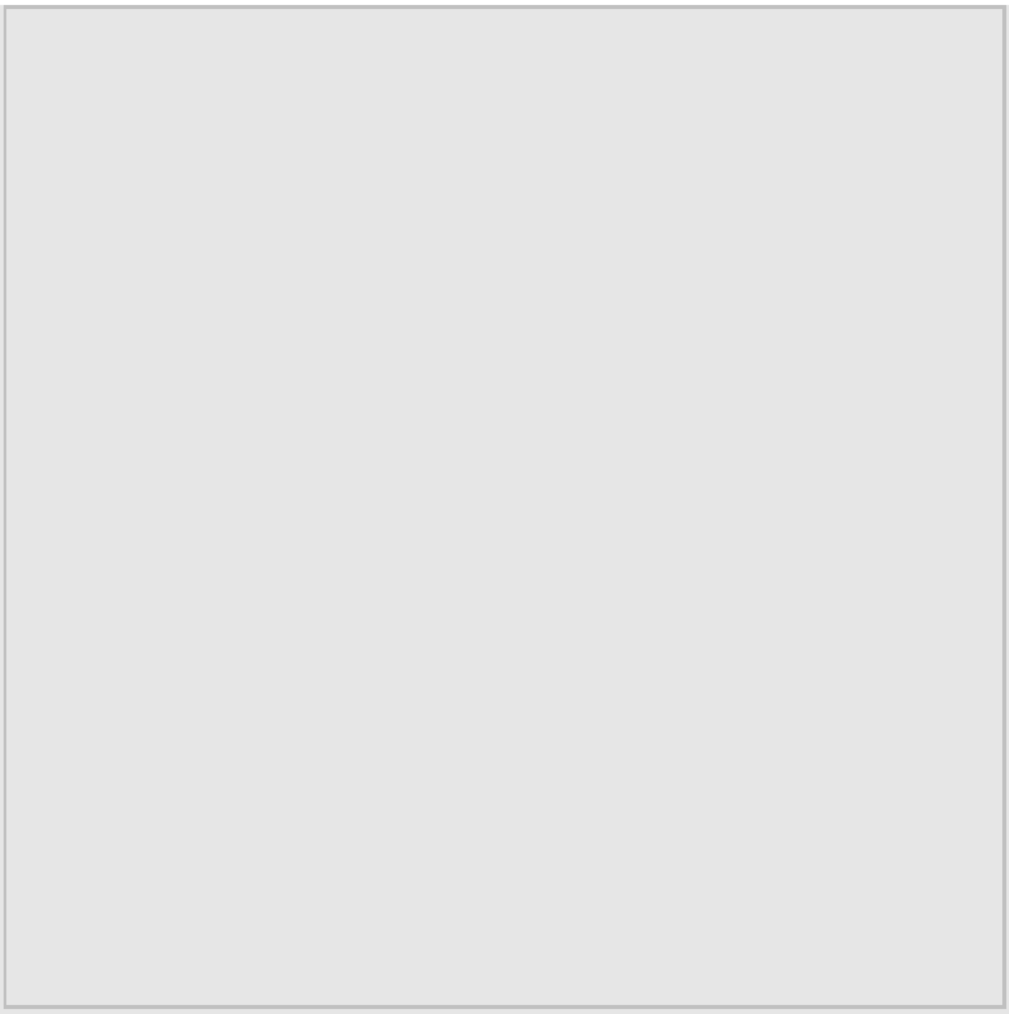
Toyota Financial Services of Japan and its insurance partner, Aioi Nissay Dowa Insurance Company, have become one of the most significant investors in the Finnish company MaaS Global, the leading developer of the Mobility-as-a-Service (MaaS) concept more...

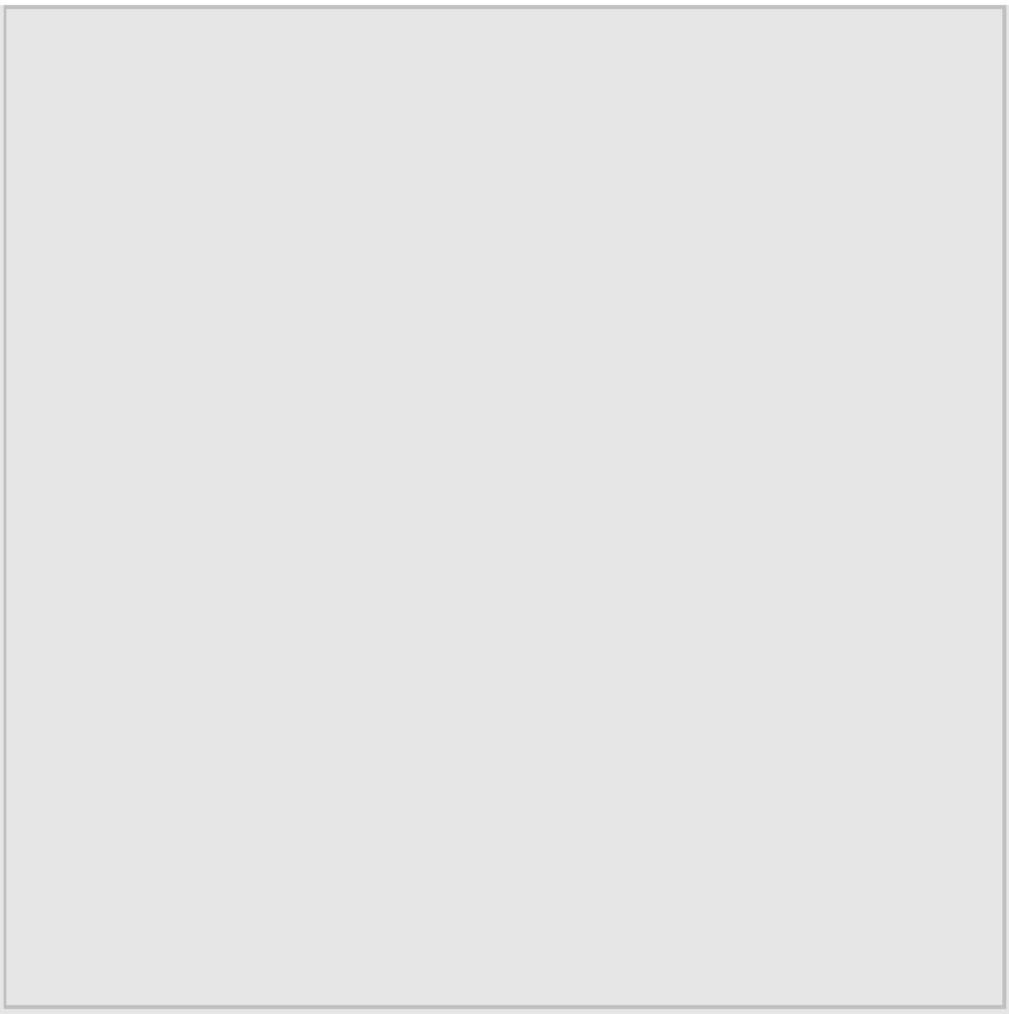
More news...

- European Commission proposes US$3bn investment for 152 transport projects
- USDOT provides US$99.6m loan for multimodal transport project in Washington State
- Road and automotive groups to advance deployment of C-ITS in Europe by 2019
- European Commission presents five Excellence in Road Safety Awards
- System uses streetlights to provide accurate, low-cost traffic counts
- Three consultancies form JV to accelerate California's I-405 Improvement Project
- Jacobs to design active traffic management system for I-76 corridor in Pennsylvania
- Moovit launches mobility data and analytics tools to improve urban transport management
- Minnesota ready to test use of autonomous buses in cold climate conditions
- NEW JOB VANCACIES: Your next career move could be here!









Inside this issue...

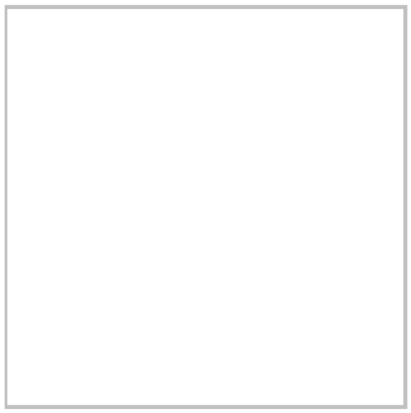


<< COVER STORY
WATCHERS AT THE WALL

What is the best way to protect your borders while processing vehicles at speed? Saul Wordsworth examines a case in point at a border crossing between the USA and Mexico, in Arizona

<< LOW EMISSION ZONES
BREATHE AGAIN

As low emission zones hit headlines across Europe, Jack Roper investigates the challenges involved in using ALPR cameras to enforce such schemes



<< INTERVIEW

JIM O'SULLIVAN

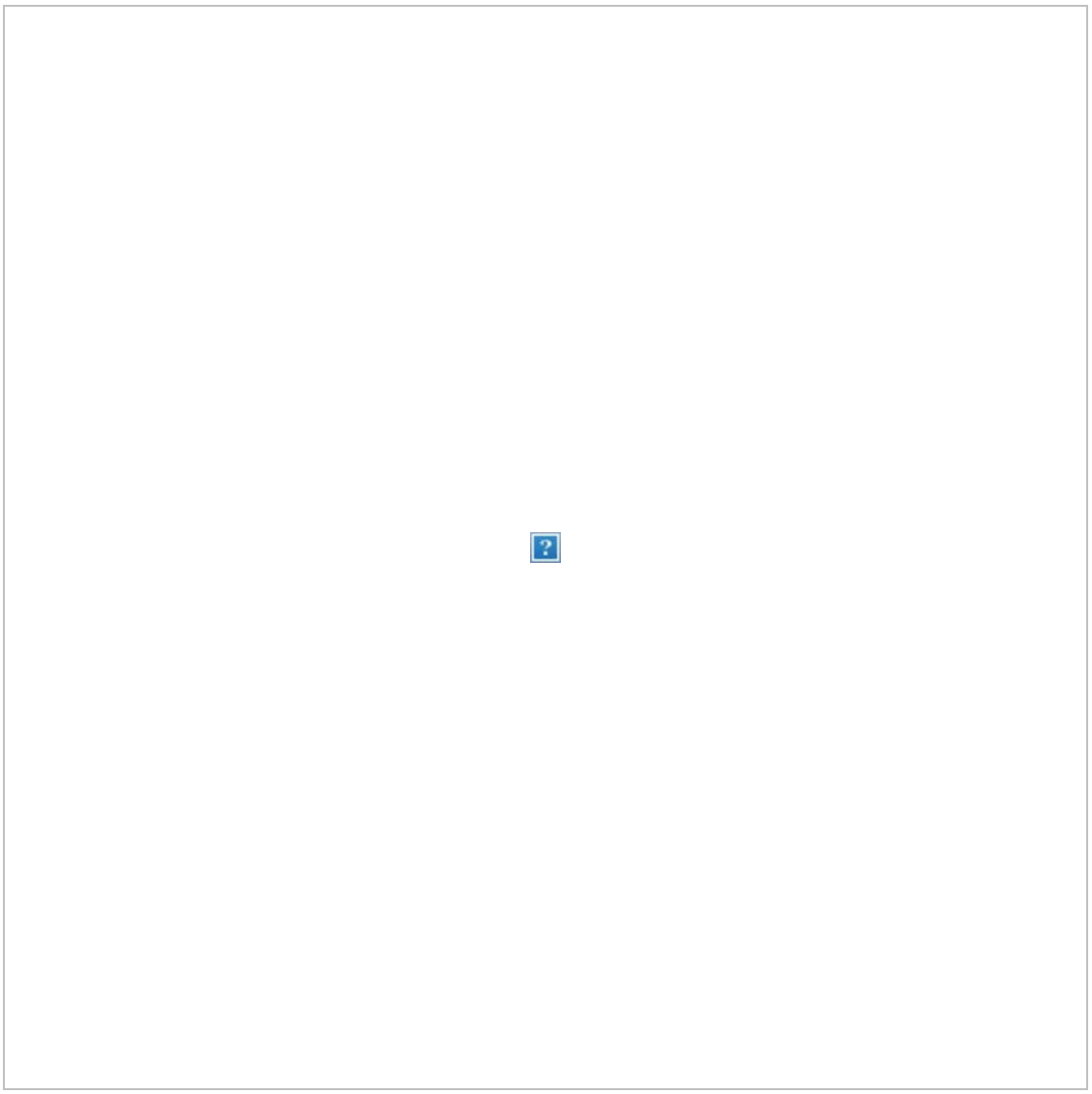
Jim O'Sullivan has enjoyed two successful years as CEO of Highways England. Now he's making plans for even greater achievements in the near future.

This email (which includes any files transmitted with it) is confidential and may also be legally privileged. It is intended solely for the use of the individual to whom it is addressed. Any views or opinions presented are solely those of the author and do not necessarily represent those of UKi Media & Events. If you are not the intended recipient, be advised that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited. If you have received this message in error, do not open any attachment but please notify the sender (above) deleting this message from your system. Please rely on your own anti-virus system, no responsibility is taken by the sender for any damage rising out of virus infection.

UKi Media & Events, a division of UKIP Media & Events Limited
Registered Address: 26 Red Lion Square, London, WC1R 4AG
VAT No. GB879 4451 71
Registration Number: 5893940
Company registered in England and Wales

From: Traffic Technology Today
To: Dowd, Timothy (POL)
Subject: USA"s first thermal-detection based, wrong-way warning system
Date: Thursday, June 15, 2017 12:02:33 PM

If you are having trouble viewing this email, click here to display it in your web browser





NEW VIDEO: New technology helps to lift unnecessary weight restrictions on bridges

VIDEO REPORT: WSDOT uses new data-driven safety analysis tools to improve road safety



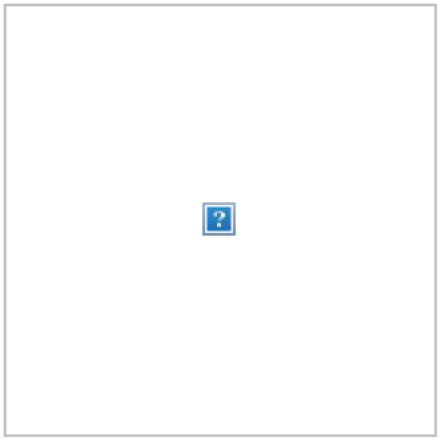
Weight restrictions on more than 60,000 bridges in the USA limit the movement of large freight and emergency vehicles. THMPER (Targeted Hits for Modal Parameter Estimation and Rating) is a new, innovative, cost-effective technology that determines a bridge's dynamic signature, enabling restrictions on some bridges to be slackened, easing traffic flow **more...**



Data-driven safety analysis (DDSA) is a collection of new tools and techniques that allows transportation agencies to better manage their funds and projects, and reduce the number of crashes involving KSIs (killed or serious injuries). This video shows how Washington State Department of Transportation (WSDOT) is making use of DDSA **more...**

For more of the latest multimedia reports visit our Video & Audio homepage here

Get involved in our weekly poll!



Last week, and for the first time **(read here)** Google shared results of a 'pollution map' it has created in Oakland, California, using its mapping vehicles. The ambition is that this map will show where improvements in air quality need to be made and make residents think twice about spending too much time in these areas. But what do you think...

What is the most effective way to protect pedestrians from pollution in our city centers?

1) Mapping
2) Low emission zones
3) Dynamic traffic management

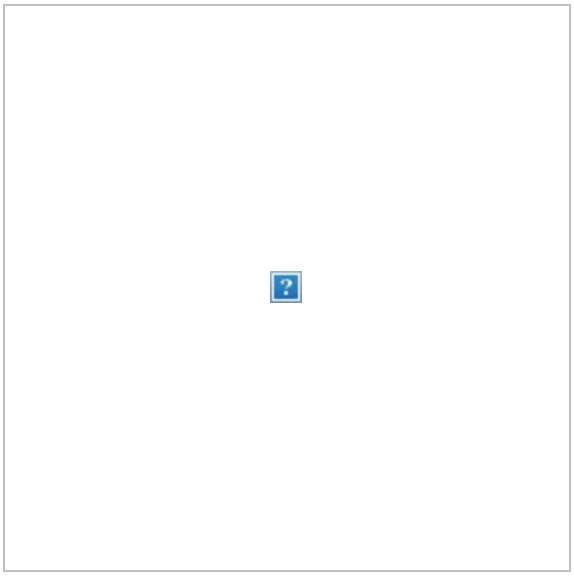
VOTE NOW to share your views

Last week, the Institute of Transportation Engineers (ITE) and partner organizations started encouraging the public to participate in its new 'Video Analytics Towards

Vision Zero' project **(read here)**, which aims to teach computers how to analyze traffic video footage in order to improve road safety. We then asked you: Is crowdsourcing a safe and effective way to 'teach' computer systems? The result was unanimous – a first in our weekly poll. All voters (100%) answered 'yes', and believe computers can safely and effectively be taught with crowdsourcing.

Also in the news this week...

Arizona to develop USA's first thermal-detection based, wrong-way warning system



Arizona's State Transportation Board has approved a US$3.7m project to construct a first-in-the-nation thermal detection system on Interstate 17, which will monitor wrong-way vehicles and alert the other drivers and law enforcement of them **more...**

>	Ford to open new Smart Mobility Innovation Office in London
>	American Center for Mobility, SAE International and ITE to fast-track CAV standards
>	Connected Signals offers free access to its traffic signal stop line data
>	Honda targeting SAE Level 4 automated driving capability by 2025
>	Sice delivers new back office system for major Australian tollway
>	Texas DOT installing new dynamic message signs in metropolitan Austin region
>	Egis to deliver incident response and maintenance for Brisbane tunnel network
>	Ramp metering to be deployed on I-287 as part of New York State's ICM project
>	New Zealand government launches Smarter Transport Pricing project
>	Dahua launches hybrid thermal camera for transport industry applications

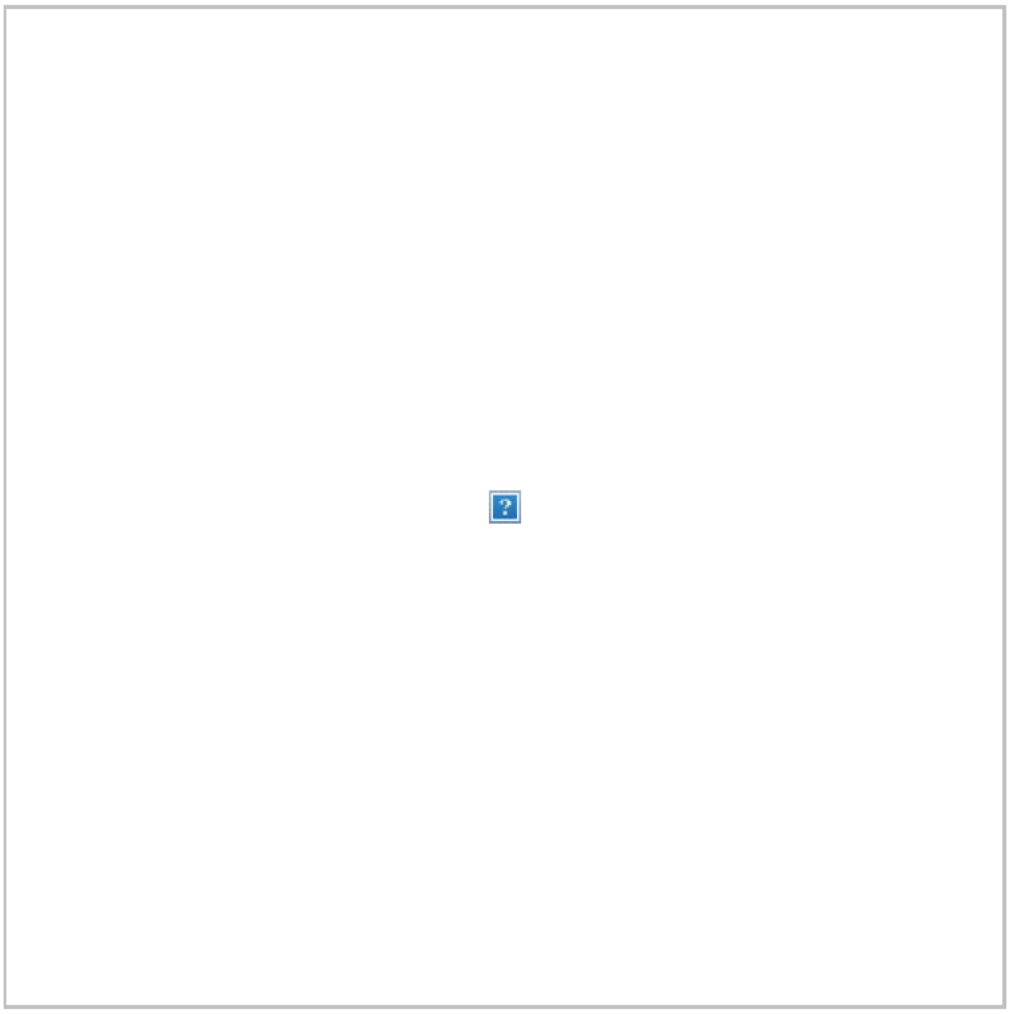
> NEW JOB VACANCIES: Your next career move could be here!











Inside this issue...



<< COVER STORY

WATCHERS AT THE WALL

What is the best way to protect your borders while processing vehicles at speed? Saul Wordsworth examines a case in point at a border crossing between the USA and Mexico, in Arizona



<<LOW EMISSION ZONES

BREATHE AGAIN

As low emission zones hit headlines across Europe, Jack Roper investigates the challenges involved in using ALPR cameras to enforce such schemes



<< INTERVIEW

JIM O'SULLIVAN

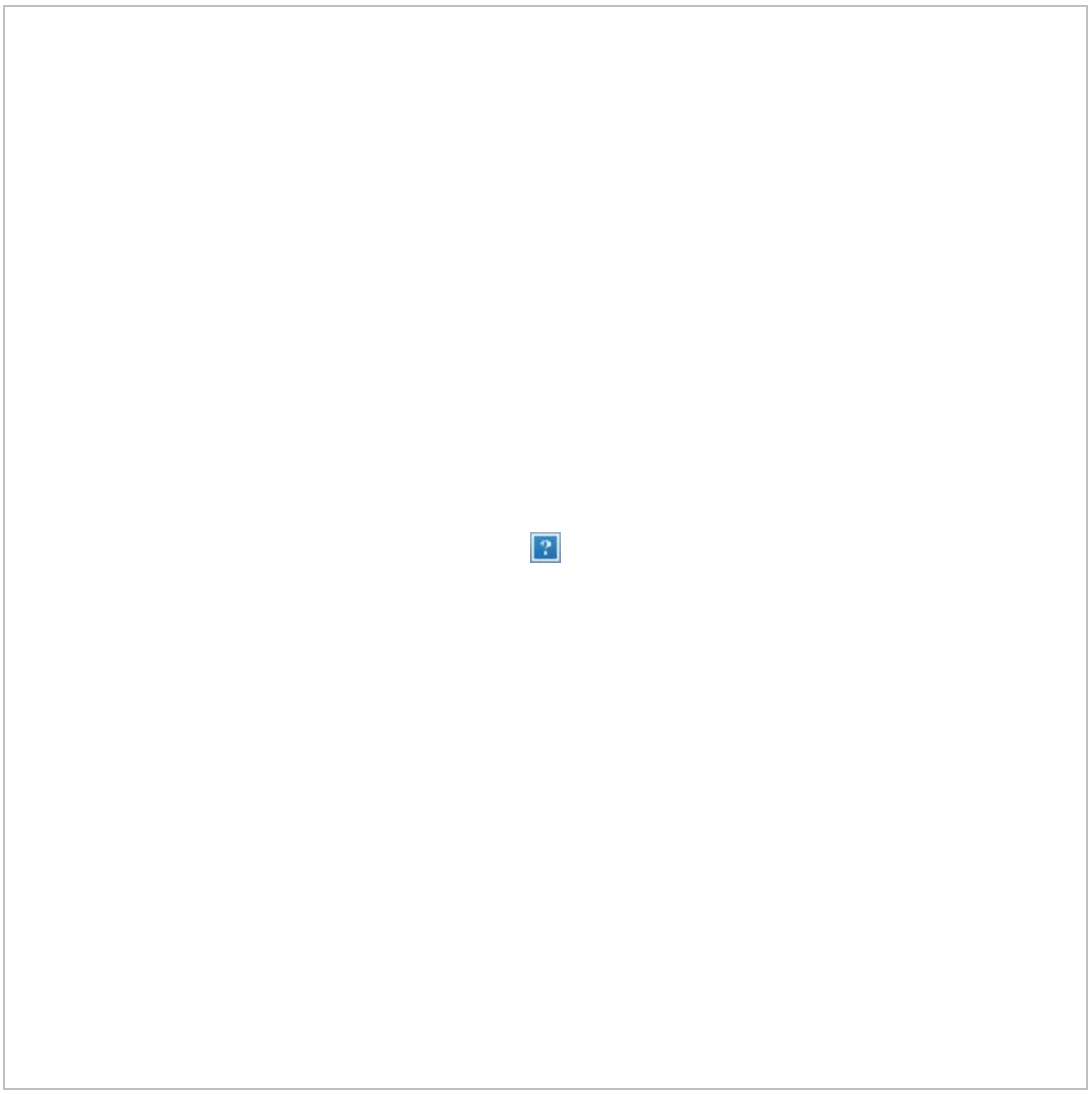
Jim O'Sullivan has enjoyed two successful years as CEO of Highways England. Now he's making plans for even greater achievements in the near future

This email (which includes any files transmitted with it) is confidential and may also be legally privileged. It is intended solely for the use of the individual to whom it is addressed. Any views or opinions presented are solely those of the author and do not necessarily represent those of UKi Media & Events. If you are not the intended recipient, be advised that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited. If you have received this message in error, do not open any attachment but please notify the sender (above) deleting this message from your system. Please rely on your own anti-virus system, no responsibility is taken by the sender for any damage rising out of virus infection.

UKi Media & Events, a division of UKIP Media & Events Limited
Registered Address: 26 Red Lion Square, London, WC1R 4AG
VAT No. GB879 4451 71
Registration Number: 5893940
Company registered in England and Wales

From: Traffic Technology Today
To: Dowd, Timothy (POL)
Subject: USA"s first thermal-detection based, wrong-way warning system
Date: Thursday, June 15, 2017 12:02:33 PM

If you are having trouble viewing this email, click here to display it in your web browser





NEW VIDEO: New technology helps to lift unnecessary weight restrictions on bridges

VIDEO REPORT: WSDOT uses new data-driven safety analysis tools to improve road safety



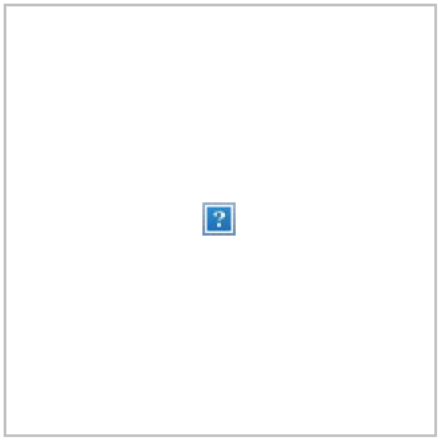
Weight restrictions on more than 60,000 bridges in the USA limit the movement of large freight and emergency vehicles. THMPER (Targeted Hits for Modal Parameter Estimation and Rating) is a new, innovative, cost-effective technology that determines a bridge's dynamic signature, enabling restrictions on some bridges to be slackened, easing traffic flow **more...**



Data-driven safety analysis (DDSA) is a collection of new tools and techniques that allows transportation agencies to better manage their funds and projects, and reduce the number of crashes involving KSIs (killed or serious injuries). This video shows how Washington State Department of Transportation (WSDOT) is making use of DDSA **more...**

For more of the latest multimedia reports visit our Video & Audio homepage here

Get involved in our weekly poll!



Last week, and for the first time **(read here)** Google shared results of a 'pollution map' it has created in Oakland, California, using its mapping vehicles. The ambition is that this map will show where improvements in air quality need to be made and make residents think twice about spending too much time in these areas. But what do you think...

What is the most effective way to protect pedestrians from pollution in our city centers?

1) Mapping
2) Low emission zones
3) Dynamic traffic management

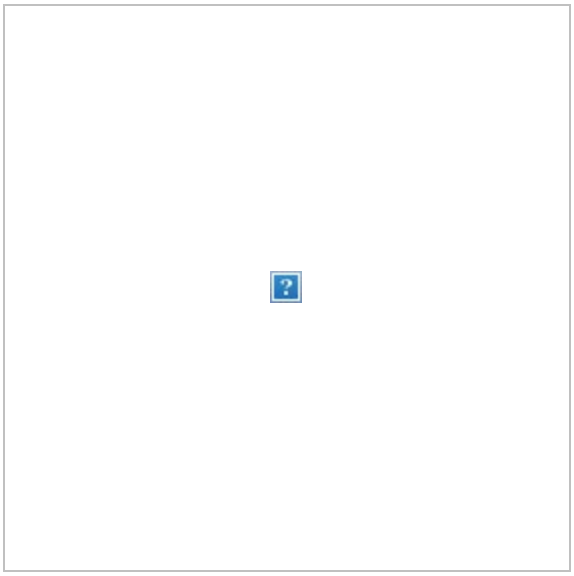
VOTE NOW to share your views

Last week, the Institute of Transportation Engineers (ITE) and partner organizations started encouraging the public to participate in its new 'Video Analytics Towards

Vision Zero' project **(read here)**, which aims to teach computers how to analyze traffic video footage in order to improve road safety. We then asked you: Is crowdsourcing a safe and effective way to 'teach' computer systems? The result was unanimous – a first in our weekly poll. All voters (100%) answered 'yes', and believe computers can safely and effectively be taught with crowdsourcing.

Also in the news this week...

Arizona to develop USA's first thermal-detection based, wrong-way warning system



Arizona's State Transportation Board has approved a US$3.7m project to construct a first-in-the-nation thermal detection system on Interstate 17, which will monitor wrong-way vehicles and alert the other drivers and law enforcement of them **more...**

>	Ford to open new Smart Mobility Innovation Office in London
>	American Center for Mobility, SAE International and ITE to fast-track CAV standards
>	Connected Signals offers free access to its traffic signal stop line data
>	Honda targeting SAE Level 4 automated driving capability by 2025
>	Sice delivers new back office system for major Australian tollway
>	Texas DOT installing new dynamic message signs in metropolitan Austin region
>	Egis to deliver incident response and maintenance for Brisbane tunnel network
>	Ramp metering to be deployed on I-287 as part of New York State's ICM project
>	New Zealand government launches Smarter Transport Pricing project
>	Dahua launches hybrid thermal camera for transport industry applications

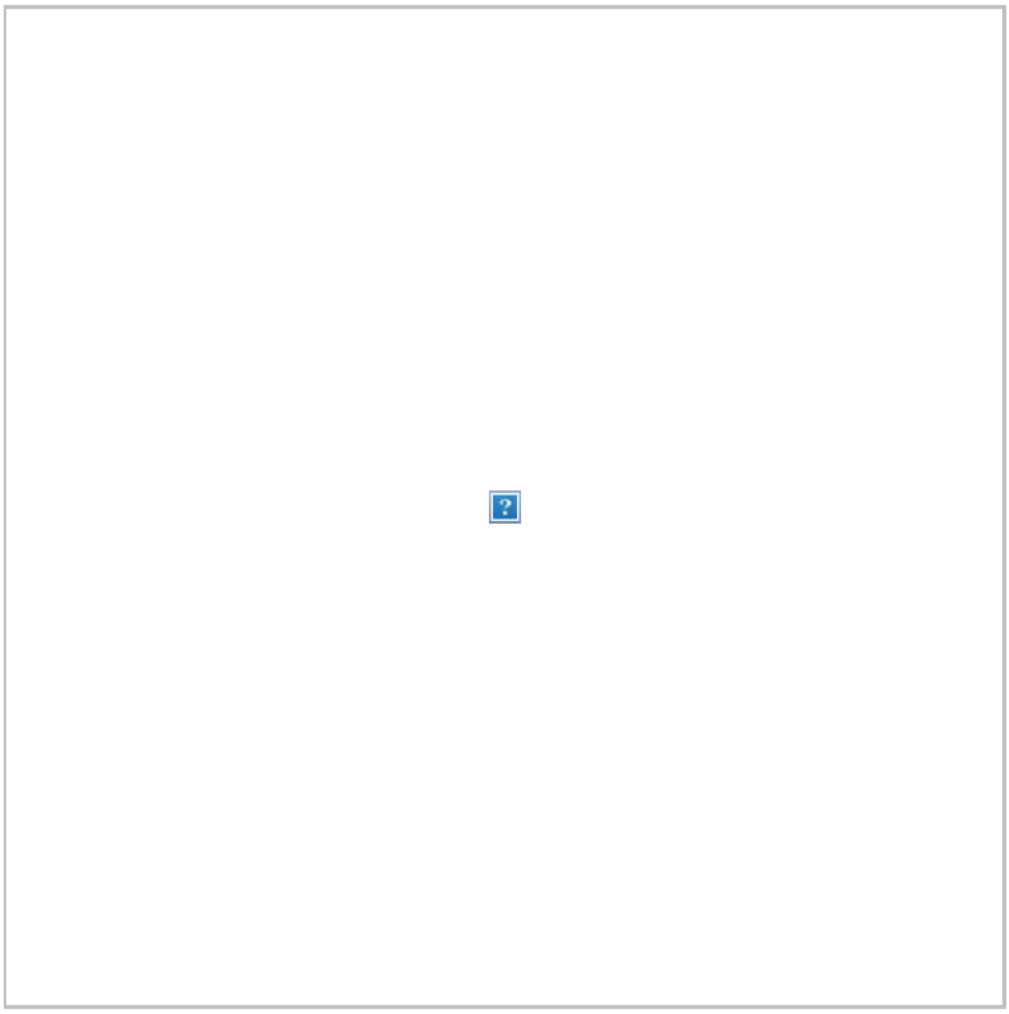
> NEW JOB VACANCIES: Your next career move could be here!











Inside this issue...



<< COVER STORY

WATCHERS AT THE WALL

What is the best way to protect your borders while processing vehicles at speed? Saul Wordsworth examines a case in point at a border crossing between the USA and Mexico, in Arizona



<<LOW EMISSION ZONES

BREATHE AGAIN

As low emission zones hit headlines across Europe, Jack Roper investigates the challenges involved in using ALPR cameras to enforce such schemes



<< INTERVIEW

JIM O'SULLIVAN

Jim O'Sullivan has enjoyed two successful years as CEO of Highways England. Now he's making plans for even greater achievements in the near future











This email (which includes any files transmitted with it) is confidential and may also be legally privileged. It is intended solely for the use of the individual to whom it is addressed. Any views or opinions presented are solely those of the author and do not necessarily represent those of UKi Media & Events. If you are not the intended recipient, be advised that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited. If you have received this message in error, do not open any attachment but please notify the sender (above) deleting this message from your system. Please rely on your own anti-virus system, no responsibility is taken by the sender for any damage rising out of virus infection.

UKi Media & Events, a division of UKIP Media & Events Limited
Registered Address: 26 Red Lion Square, London, WC1R 4AG
VAT No. GB879 4451 71
Registration Number: 5893940
Company registered in England and Wales

From: Traffic Technology Today
To: Dowd, Timothy (POL)
Subject: USDOT launches new infrastructure funding program
Date: Friday, July 7, 2017 5:15:38 AM

If you are having trouble viewing this email, click here to display it in your web browser

NEW VIDEO: GATEway and Ocado Technology trial driverless grocery deliveries

The TRL-led GATEway Project and Ocado Technology (a division of the online-only supermarket) have completed the UK's first trials of a self-driving grocery delivery van in the Royal Borough of Greenwich in London. This video shows an autonomous 'CargoPod' vehicle in action more...

NEW AUDIO: Hot lanes investment is helping Virginia to future-proof

In this clip, Aubrey Layne, Virginia's secretary of transportation talks with Transportation Radio's Bernie Wagenblast about how the state is banking on its investment in hot lanes, as well as being an area for new traffic technologies to be tried and tested in. He also explains how his role involves working with NASA more...

Weekly poll

This week, the US Department of Transportation (USDOT) launched a new funding program (read more here) that will make US$1.5bn available to infrastructure projects. At least 25% of this funding will be awarded to rural projects. Now, we want to know what you think…

Do you agree that funding for rural infrastructure projects should be prioritized over other types of infrastructure projects?

- **Yes**
- **No**

Click here to vote now!

Poll results

Last week, the University of Connecticut's interactive, publicly-available crash database received increasing amounts of interest at a nationwide level (full report here). We then asked you…

Although sharing data is useful, is it necessary for sensitive information, such as details of crashes, to be made available to the public? You answered…

In the news this week

Ultra Fairwood to build the world's largest autonomous vehicle transportation system in the UAE

Ultra Fairwood has signed a contract to build the world's largest autonomous electric vehicle transportation system, which will operate in Ajman City in the United Arab Emirates. The project will create a city-wide integrated transportation system that will feature a combination of PRT (personal rapid transit) and GRT (group rapid transit) vehicles
more...

More news...

TRIP report finds USA's rural roads need urgent repairs, modernization and upgrades

Government launches new transport investment plan for UK

Mediamobile and Foreca partnership to deliver V-Traffic road weather information

Las Vegas partners with Numina and Motionloft on pedestrian safety projects

Volkswagen to equip its vehicles with V2X communication technology from 2019

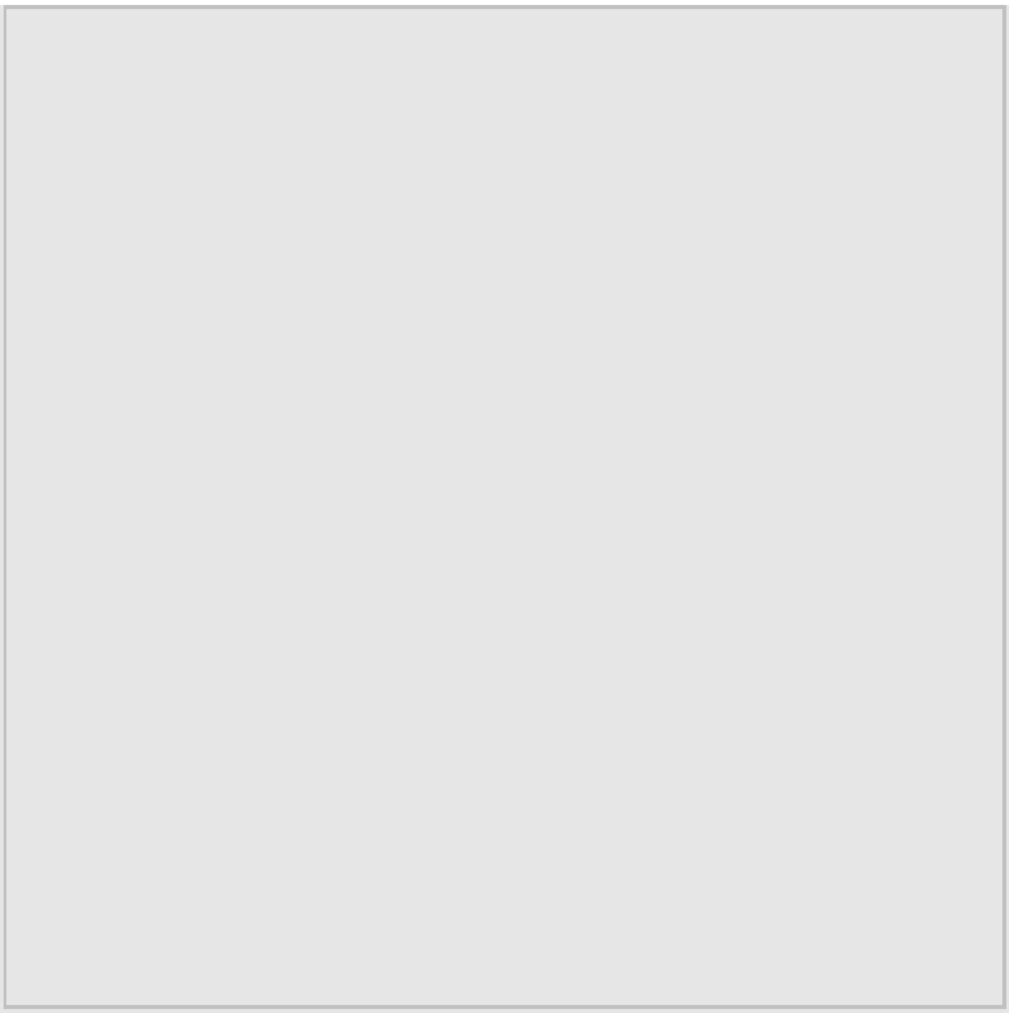
UK government announces £6.1bn program of upgrades to major roads and motorways

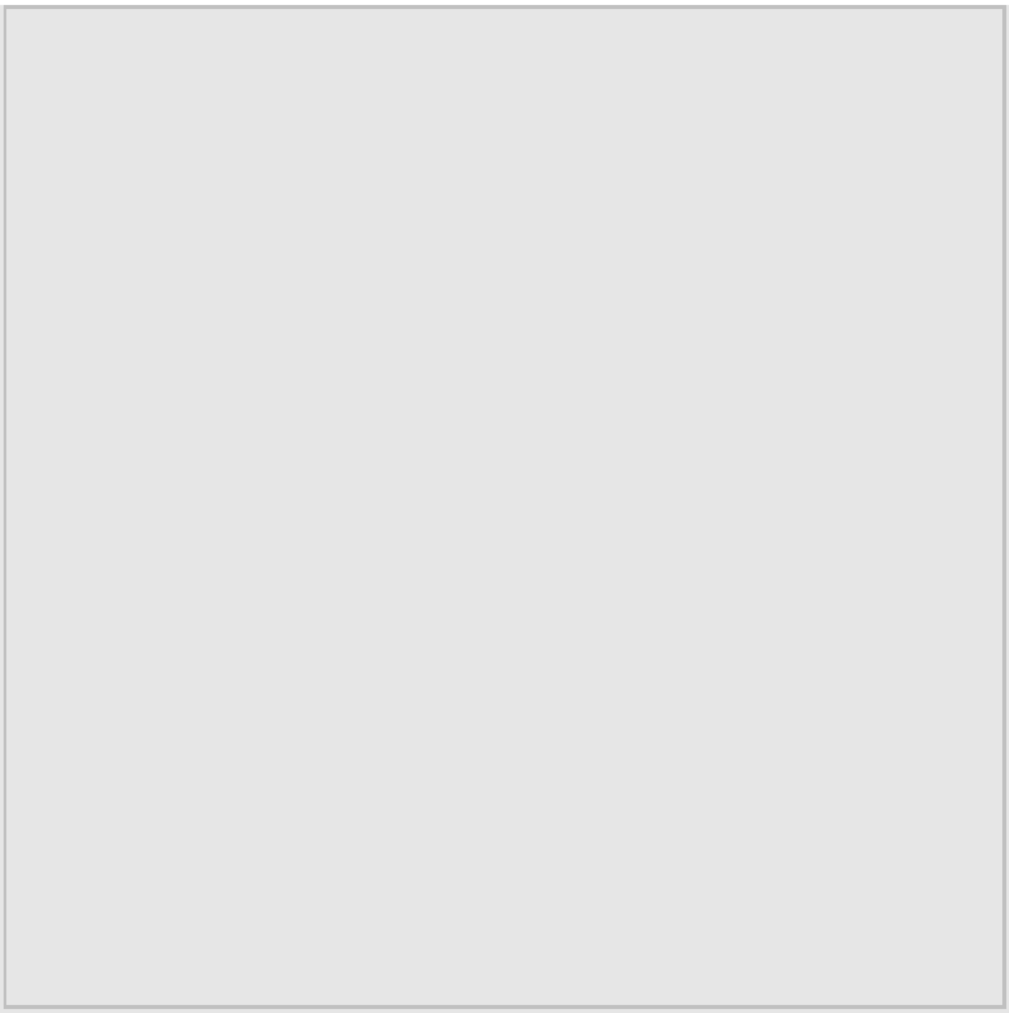
OpenDataSoft partners with Waze to offer cities improved transport network insights

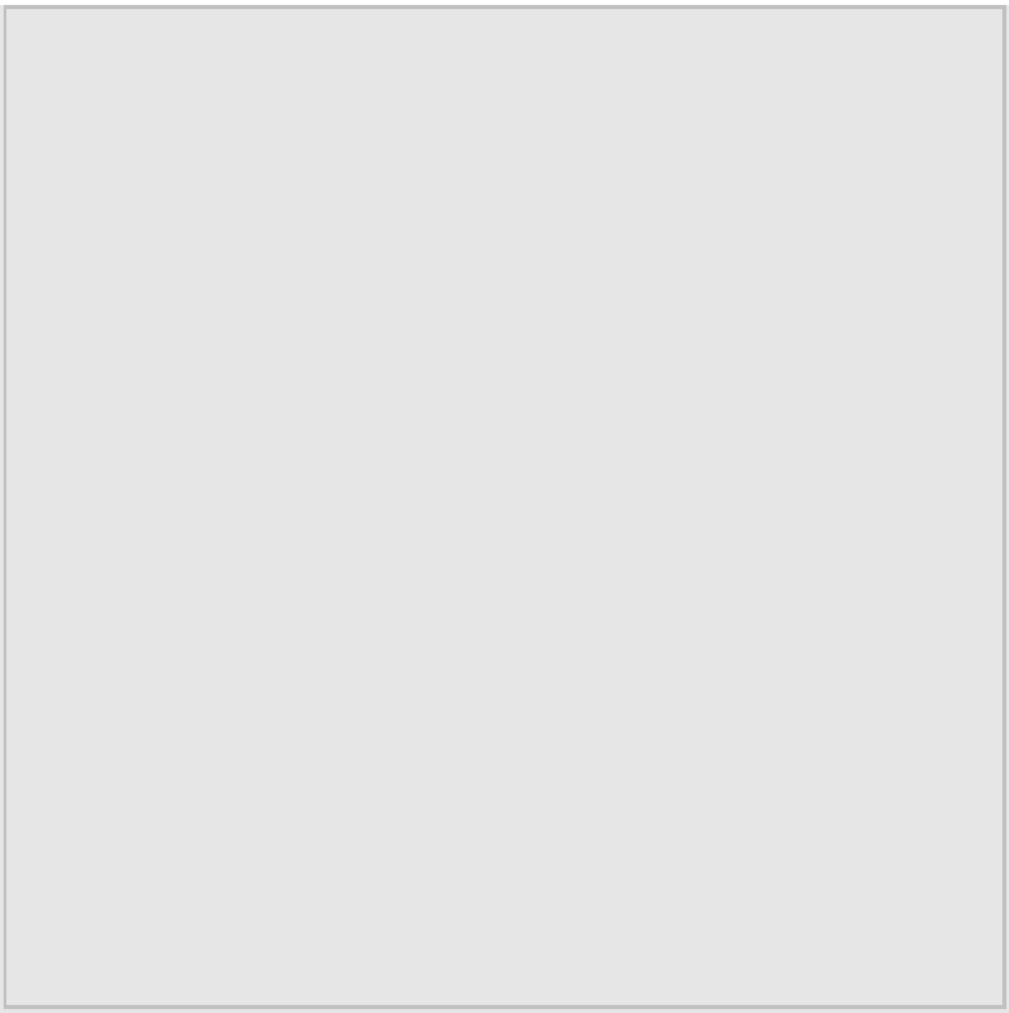
Five states win in America's Transportation Awards western region contest

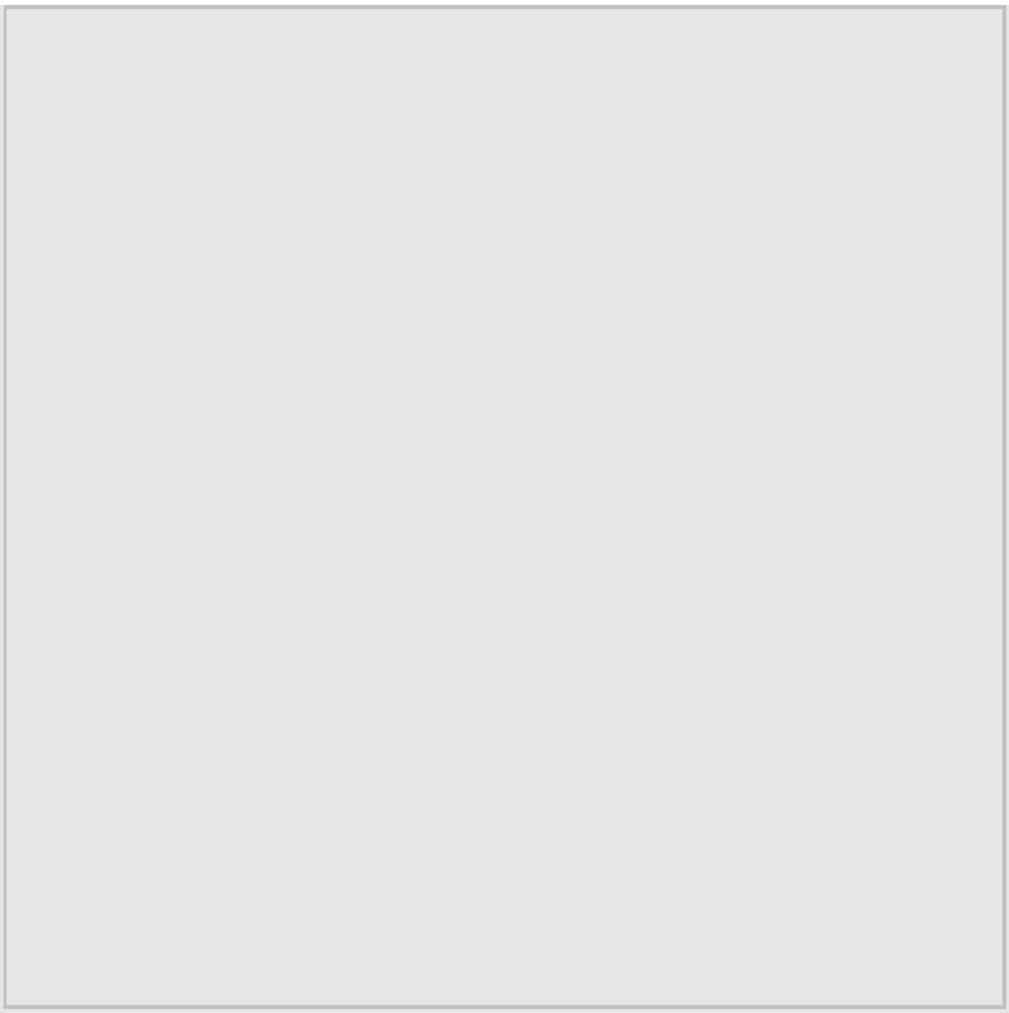
European InterCor project to start testing international interoperability of C-ITS services

NEW JOB VANCACIES: Your next career move could be here!









Inside this issue...



<< COVER STORY

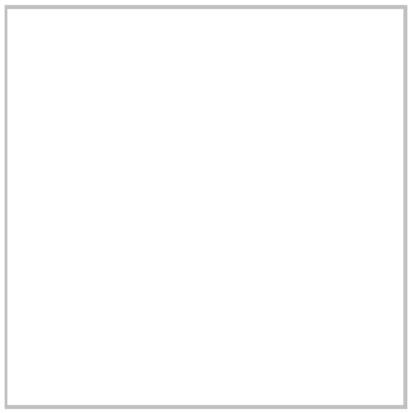
WATCHERS AT THE WALL

What is the best way to protect your borders while processing vehicles at speed? Saul Wordsworth examines a case in point at a border crossing between the USA and Mexico, in Arizona

<< LOW EMISSION ZONES

BREATHE AGAIN

As low emission zones hit headlines across Europe, Jack Roper investigates the challenges involved in using ALPR cameras to enforce such schemes



<< INTERVIEW

JIM O'SULLIVAN

Jim O'Sullivan has enjoyed two successful years as CEO of Highways England. Now he's making plans for even greater achievements in the near future.

This email (which includes any files transmitted with it) is confidential and may also be legally privileged. It is intended solely for the use of the individual to whom it is addressed. Any views or opinions presented are solely those of the author and do not necessarily represent those of UKi Media & Events. If you are not the intended recipient, be advised that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited. If you have received this message in error, do not open any attachment but please notify the sender (above) deleting this message from your system. Please rely on your own anti-virus system, no responsibility is taken by the sender for any damage rising out of virus infection.

UKi Media & Events, a division of UKIP Media & Events Limited
Registered Address: 26 Red Lion Square, London, WC1R 4AG
VAT No. GB879 4451 71
Registration Number: 5893940
Company registered in England and Wales

From: Traffic Technology Today
To: Dowd, Timothy (POL)
Subject: USDOT launches new infrastructure funding program
Date: Friday, July 7, 2017 5:15:42 AM

If you are having trouble viewing this email, click here to display it in your web browser

NEW VIDEO: GATEway and Ocado Technology trial driverless grocery deliveries

The TRL-led GATEway Project and Ocado Technology (a division of the online-only supermarket) have completed the UK's first trials of a self-driving grocery delivery van in the Royal Borough of Greenwich in London. This video shows an autonomous 'CargoPod' vehicle in action more...

NEW AUDIO: Hot lanes investment is helping Virginia to future-proof

In this clip, Aubrey Layne, Virginia's secretary of transportation talks with Transportation Radio's Bernie Wagenblast about how the state is banking on its investment in hot lanes, as well as being an area for new traffic technologies to be tried and tested in. He also explains how his role involves working with NASA more...

Weekly poll

This week, the US Department of Transportation (USDOT) launched a new funding program (read more here) that will make US$1.5bn available to infrastructure projects. At least 25% of this funding will be awarded to rural projects. Now, we want to know what you think…

Do you agree that funding for rural infrastructure projects should be prioritized over other types of infrastructure projects?

- **Yes**
- **No**

Click here to vote now!

Poll results

Last week, the University of Connecticut's interactive, publicly-available crash database received increasing amounts of interest at a nationwide level (full report here). We then asked you…

Although sharing data is useful, is it necessary for sensitive information, such as details of crashes, to be made available to the public? You answered…

In the news this week

Ultra Fairwood to build the world's largest autonomous vehicle transportation system in the UAE

Ultra Fairwood has signed a contract to build the world's largest autonomous electric vehicle transportation system, which will operate in Ajman City in the United Arab Emirates. The project will create a city-wide integrated transportation system that will feature a combination of PRT (personal rapid transit) and GRT (group rapid transit) vehicles
more...

More news...

TRIP report finds USA's rural roads need urgent repairs, modernization and upgrades

Government launches new transport investment plan for UK

Mediamobile and Foreca partnership to deliver V-Traffic road weather information

Las Vegas partners with Numina and Motionloft on pedestrian safety projects

Volkswagen to equip its vehicles with V2X communication technology from 2019

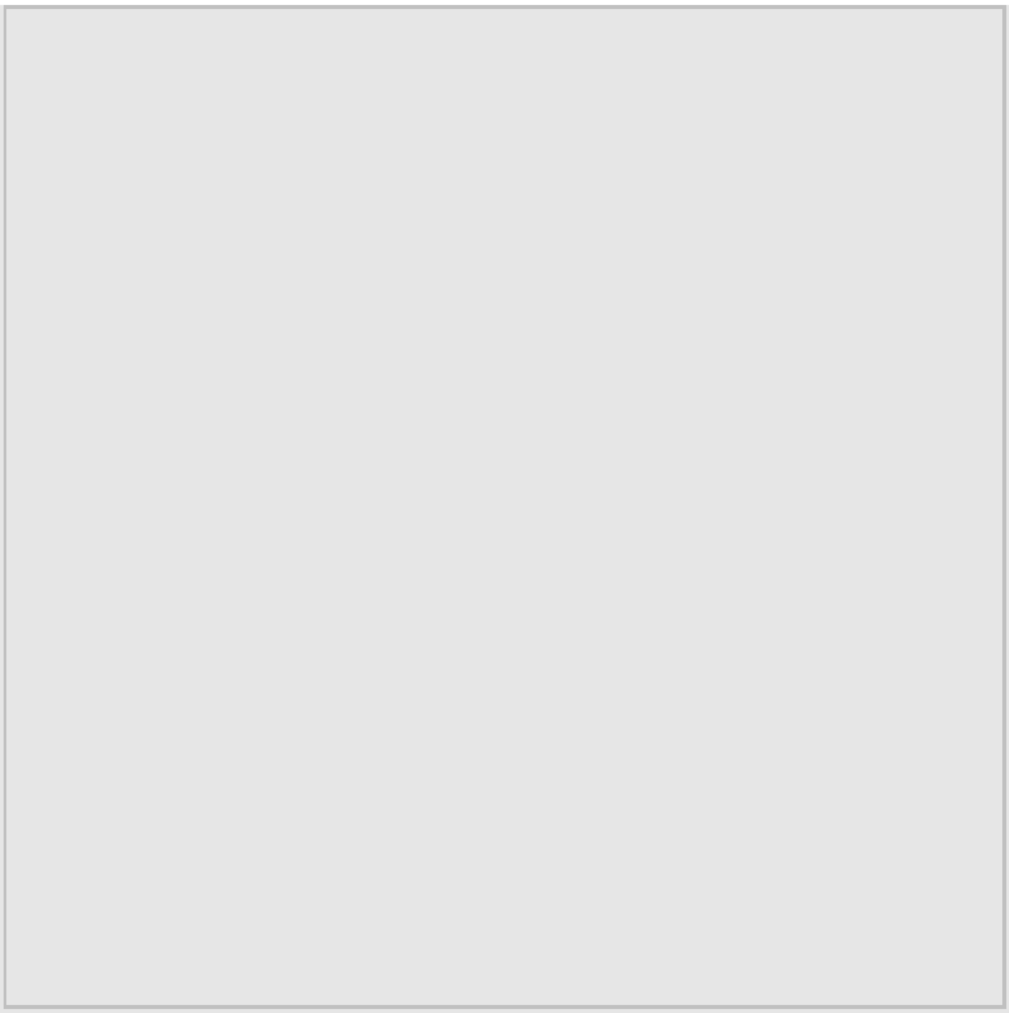
UK government announces £6.1bn program of upgrades to major roads and motorways

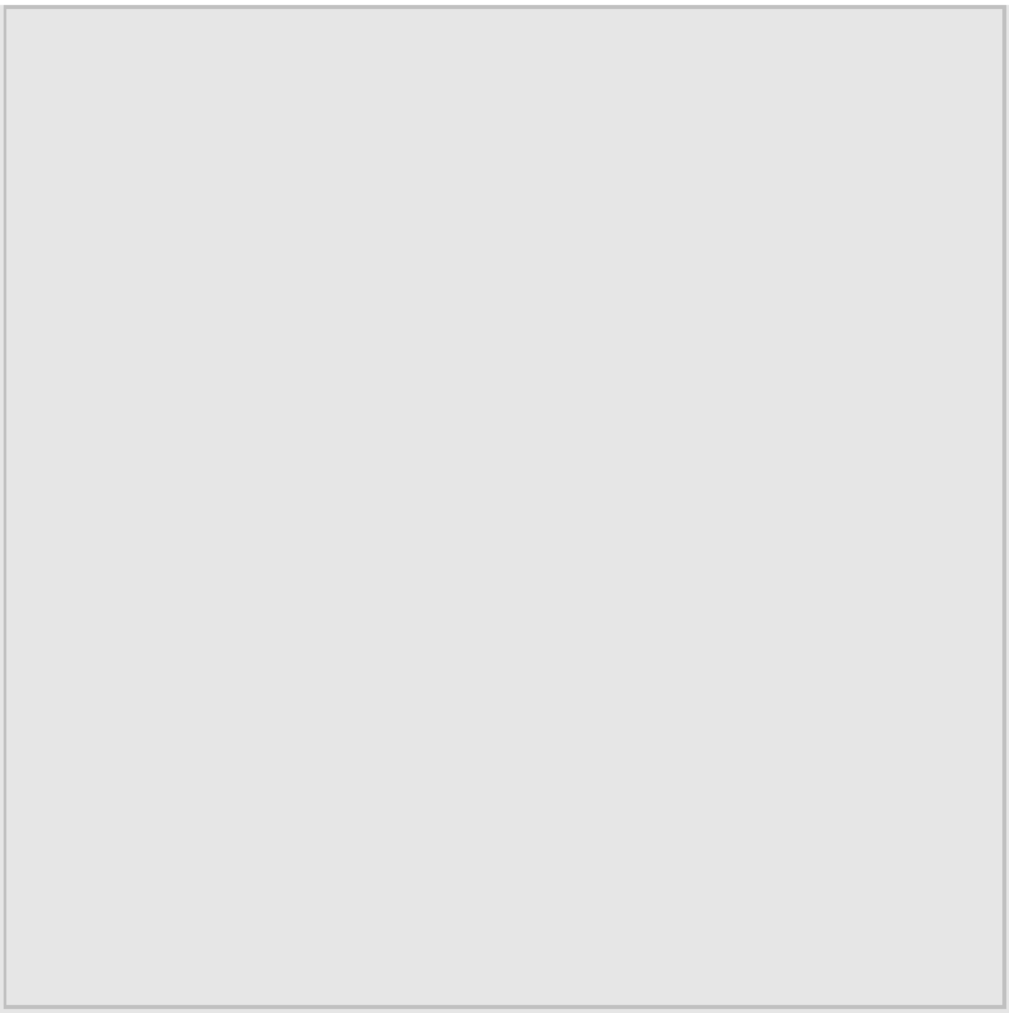
OpenDataSoft partners with Waze to offer cities improved transport network insights

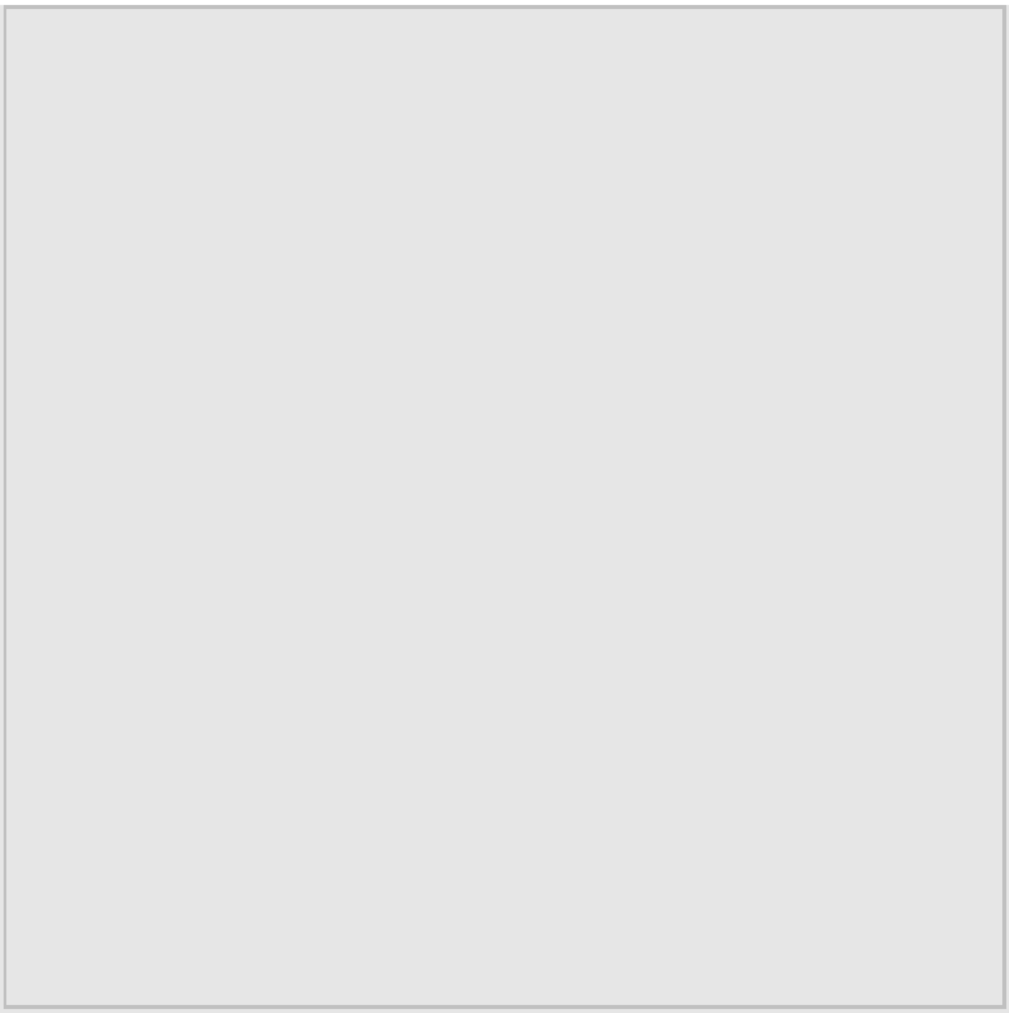
Five states win in America's Transportation Awards western region contest

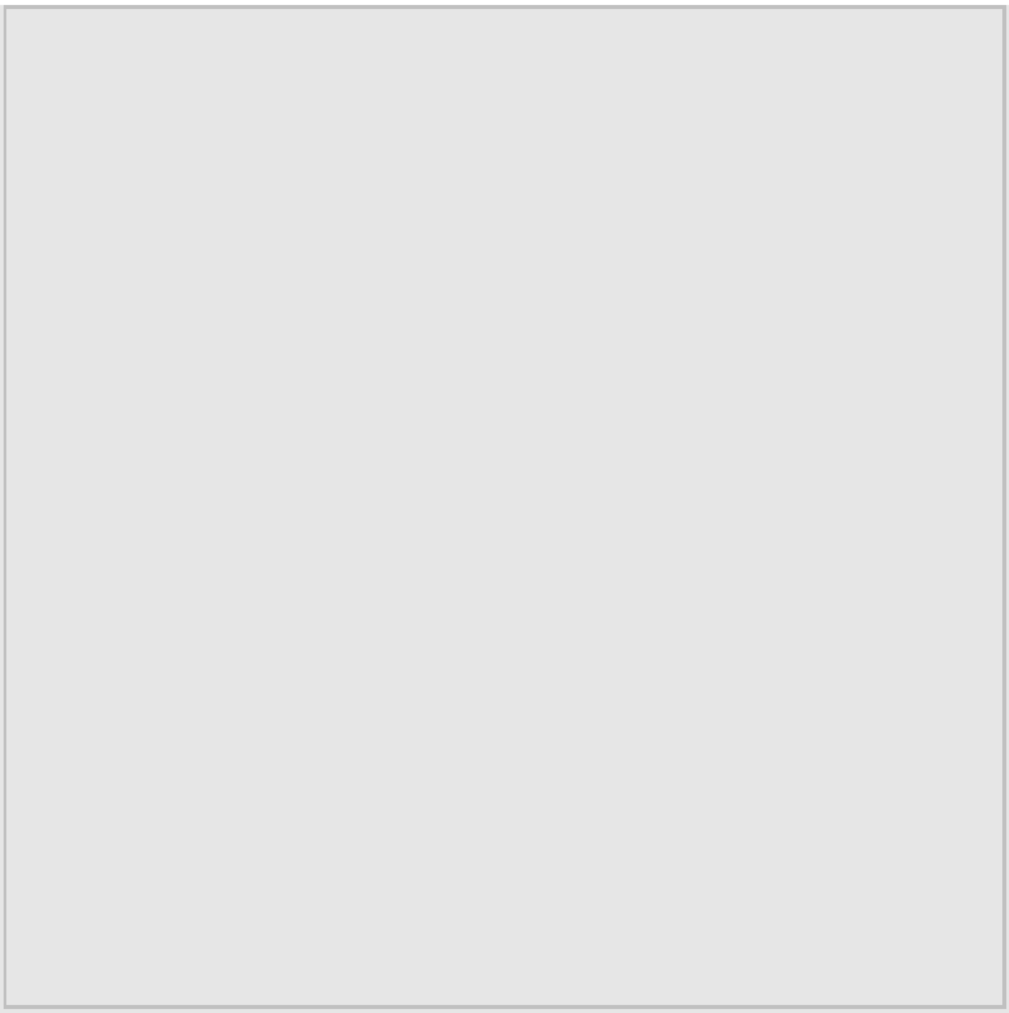
European InterCor project to start testing international interoperability of C-ITS services

NEW JOB VANCACIES: Your next career move could be here!









Inside this issue...

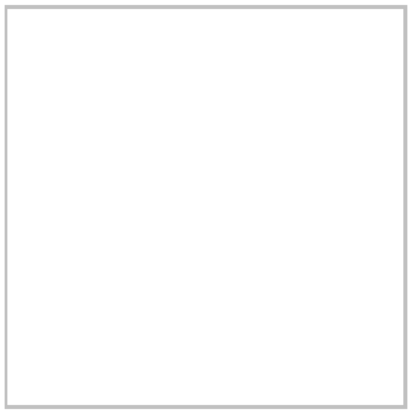


<< COVER STORY
WATCHERS AT THE WALL

What is the best way to protect your borders while processing vehicles at speed? Saul Wordsworth examines a case in point at a border crossing between the USA and Mexico, in Arizona

<< LOW EMISSION ZONES
BREATHE AGAIN

As low emission zones hit headlines across Europe, Jack Roper investigates the challenges involved in using ALPR cameras to enforce such schemes



<< INTERVIEW

JIM O'SULLIVAN

Jim O'Sullivan has enjoyed two successful years as CEO of Highways England. Now he's making plans for even greater achievements in the near future.

This email (which includes any files transmitted with it) is confidential and may also be legally privileged. It is intended solely for the use of the individual to whom it is addressed. Any views or opinions presented are solely those of the author and do not necessarily represent those of UKi Media & Events. If you are not the intended recipient, be advised that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited. If you have received this message in error, do not open any attachment but please notify the sender (above) deleting this message from your system. Please rely on your own anti-virus system, no responsibility is taken by the sender for any damage rising out of virus infection.

UKi Media & Events, a division of UKIP Media & Events Limited
Registered Address: 26 Red Lion Square, London, WC1R 4AG
VAT No. GB879 4451 71
Registration Number: 5893940
Company registered in England and Wales

From: Griffin, Daniel (POL)
To: Eldridge, Kimberly (POL)
Subject: User manual
Date: Friday, February 10, 2017 9:42:10 AM
Attachments: BOSS_3.2x_User_Manual_final.pdf
image001.png

☺

Lieutenant Daniel J. Griffin 1129
Massachusetts State Police
Traffic Programs Section
General Headquarters
470 Worcester Rd
Framingham, Ma. 01702
508-988-7404
daniel.griffin@massmail.state.ma.us

From: Griffin, Daniel (POL)
To: Eldridge, Kimberly (POL)
Subject: User manual
Date: Friday, February 10, 2017 9:42:14 AM
Attachments: BOSS_3.2x_User_Manual_final.pdf
image001.png

☺

Lieutenant Daniel J. Griffin 1129
Massachusetts State Police
Traffic Programs Section
General Headquarters
470 Worcester Rd
Framingham, Ma. 01702
508-988-7404
daniel.griffin@massmail.state.ma.us