

LPR ASSIGNMENTS

FIXED

MOBILE (Detachment/Unit)

Fort McHenry Tunnel	Hatem Bridge
BWI/TM Airport	Tunnel Command
William Preston Lane Bridge	Francis Scott Key Bridge
Francis Scott Key Bridge	Port
	William Preston Lane Bridge
	Harry W. Nice Bridge
	Special Operations (4 units)
	BWI/ TM Airport
	Inter County Connector
	Commercial Vehicle Safety Unit (2 units)
Total - 4	Total - 14



Maryland
Transportation
Authority

ELSAG License Plate Reader Fort McHenry Tunnel installation Current

Business Owner: Police

Operation Center for Reading Systems (OCRS) 3.6.7
Operation Center Database (OCD) 3.6.6
Operation Center Web Application (OCW) 2.12.2

Back Office 3.3.4.1

- * Remote Data Collector (RDC)
- * Remove Data Manager (RMC)
- * White Hot List Importer (WHI)
- * Long Range Node (only mobile)
- * CAS Car Service (only mobile)
- * XML Exporter

Peripheral Process (PEP) 3.3.4.1

Cartography Server 1.2.3

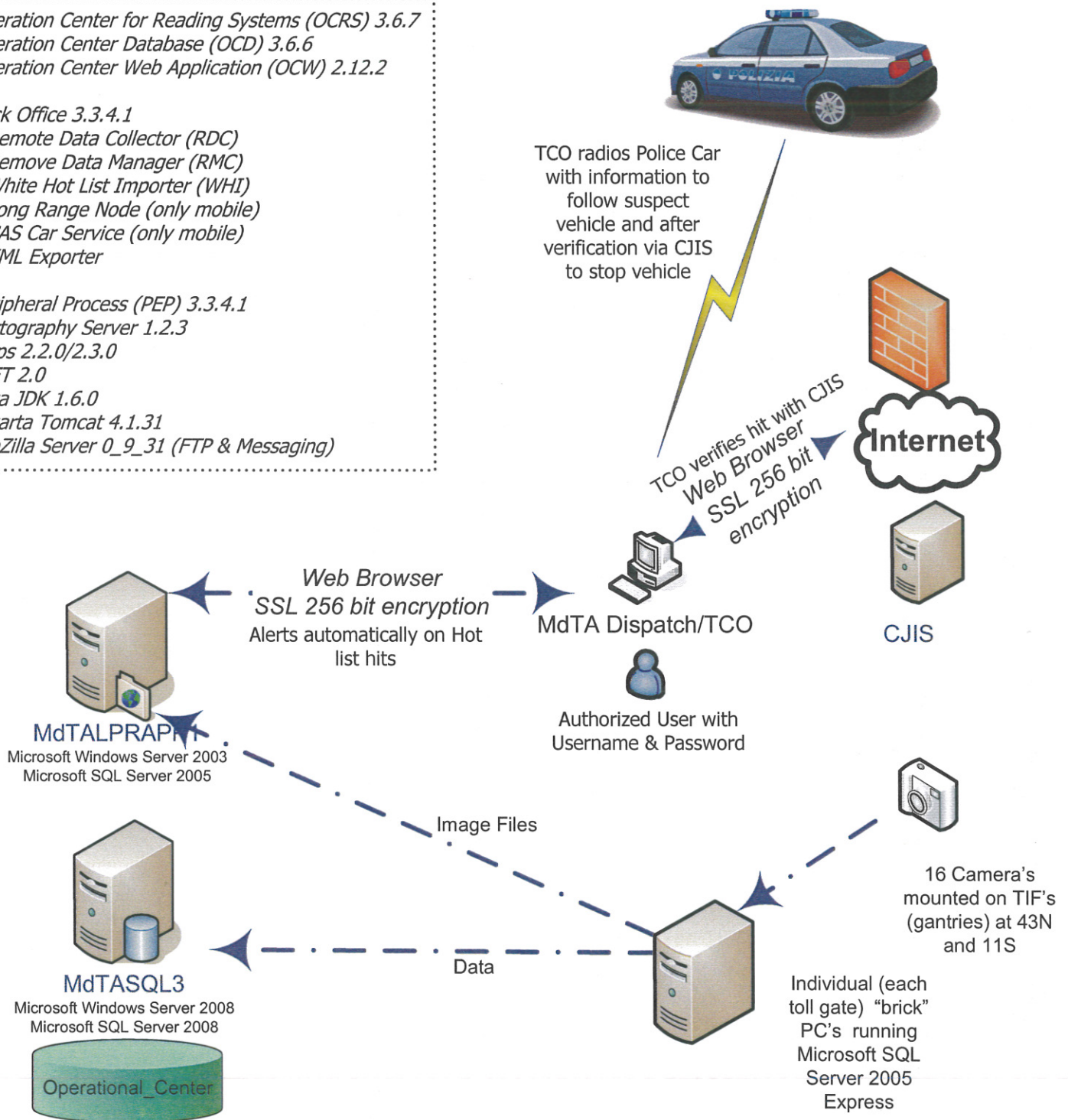
Maps 2.2.0/2.3.0

.NET 2.0

Java JDK 1.6.0

Jakarta Tomcat 4.1.31

FileZilla Server 0_9_31 (FTP & Messaging)



Source: Operation Center Installation Guide V4, CCR 2944

Server Name indicates Virtual Server in VMWare Environment

Update: 12/09/2011 DStewart

MdTA Sensitive Information

Page 49 removed - drawing contained network addresses which are security sensitive.

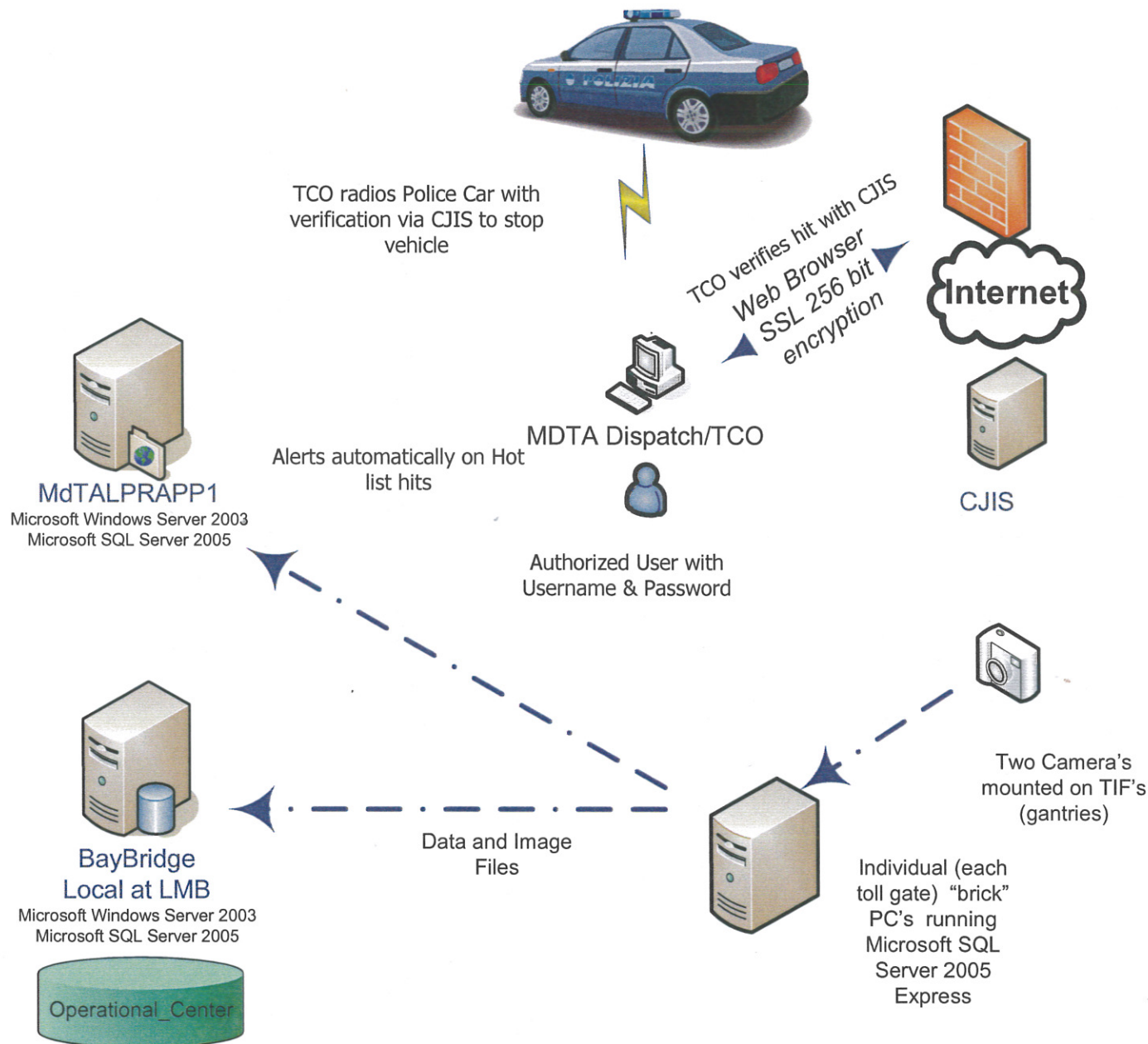
Page 48



Maryland
Transportation
Authority

ELSAG License Plate Reader
Lane Memorial Bridge installation
Current

Business Owner: Police

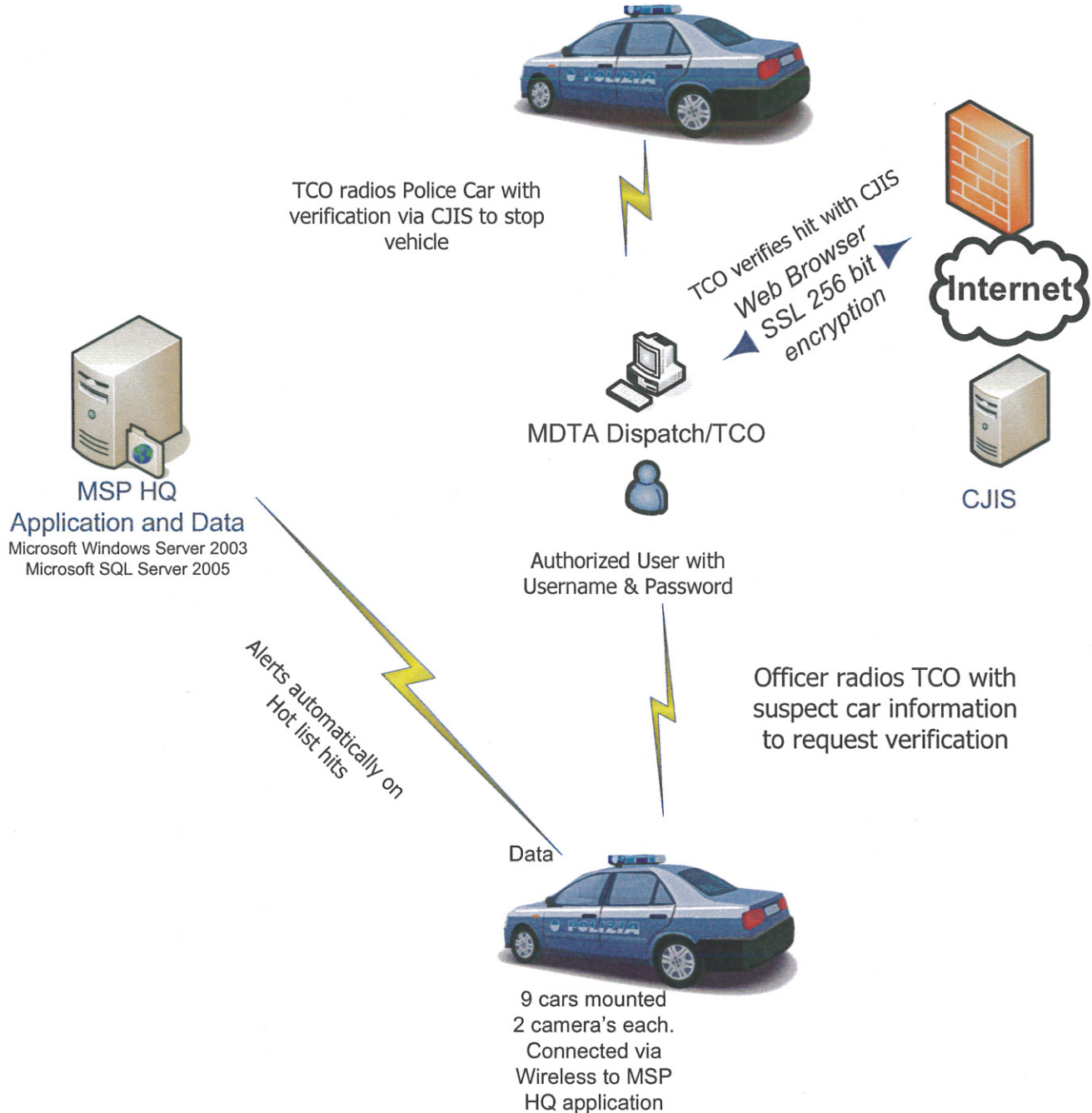


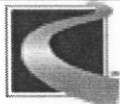


Maryland
Transportation
Authority

ELSAG Mobile License Plate Reader
In car installation
Current

Business Owner: Police





Maryland
Transportation
Authority

Mobile License Plate Reader (ALPR)

Document #:
Assigned by Budget &
Planning

**Original
Approval Date:**
05/10/11

**Revised
Approval Date:**

MDTA Police

Purpose **Procedure** **References** **Other Divisions Impacted** **Contact Information** **Procedure Status** **DFD**

Important Note: It is the responsibility of anyone using this SOP to ensure that he/she has the most current version.

Purpose

The purpose of this document is to outline the policies and procedures that govern the use of the Mobile License Plate Readers (ALPR) that have been deployed to various patrol units. The cameras capture the image of front or rear license plates.

The system utilizes technology that matches the license plates of passing vehicles against a database of stolen vehicles, stolen registration plates and vehicles sought in connection with felony investigations. The database can also include the information of vehicles wanted for other violations (Amber, Silver & Blue alerts) and will also support the purposes of Homeland Security.

This document contains the following processes: System Deployment, Security Protocol, Data Collection, Retention & Dissemination, TCO Responsibilities, Emergency Operations, Patrol Applications and Terrorist/Gang Watch lists and Scofflaw Procedures.

Applicability:

This procedure is applicable to the MDTA Police, MDTA Police Communications and E-Z Pass® (scofflaw).

Responsibility:

LPR Administrator - (Detective Division Commander, ITLE Unit designee, Detachment Commander or designee) Responsibilities outlined in section 3.

Police Shift Supervisor – Responsibilities outlined in section 6.

TCO – Responsibilities outlined in sections 4 and 6.

Patrol Officer (Operator) - Responsibilities outlined in sections 2 – 7.

Detachment Commander – Responsibilities outlined in section 1. Also, ensure that all employees are made aware of this document and that they adhere to this SOP.

Equipment:

MPH-900X2 Mobile License Plate Reader – Includes LPR Processor, 4 cameras (2 color and 2 infrared LPR in two enclosures), cables, related software and magnetized trunk mount brackets.

1. System Deployment

ALPRs are assigned to the Electronic Toll Enforcement Unit, Aggressive Driving Unit and other Units/Detachments as determined by the Commander of the Patrol Division. ALPRs assigned to individual Units/Detachments shall be assigned to personnel and used in a patrol function at the discretion of the Unit/Detachment Commander.

2. Security Protocol

The NCIC information, known as the "hotlist" is automatically uploaded to ALPR units as long as an internet connection is available on the Mobile Data Computer (MDC). The "hotlist" is sent wirelessly by the Maryland Crime Analysis Center (MCAC). The ALPR operator shall confirm, upon initial log on, that the hotlist has been uploaded by: opening the "Car System" application on the MDC desktop. The modified date should reflect the current date and time updated. The hotlist updates at 0700 and 1900 hours daily and if the automatic download did not occur, the ITLE Unit Commander or designee shall be notified.

3. Data Collection, Retention and Dissemination

- A. Via wireless connectivity MCAC will be capable of querying all system data collected by the Agency's ALPRs. Information will also be stored locally on the corresponding MDC for 35 days.
- B. Only trained personnel approved by an LPR Administrator may access system data in the MDC.
- C. All ALPR system data shall be stored locally no longer than 35 days prior to purging unless it has become, or it is reasonable to believe that it will become, evidence in a specific criminal or civil action. Evidentiary value in a criminal case includes both evidence that will inculcate or exculpate a suspect.
- D. In those circumstances when data is identified as having evidentiary value, the Detective Division Commander (or designee) or Detachment Commander (or designee) specific to the incident will review the facts of the related case and determine if the data should be saved. If it is determined that the data has evidentiary value, the appropriate commander (or designee) specific to the incident will authorize the downloading of the applicable data from the MDC onto a CD or other portable storage device.
- E. This authorization will be documented on a Supplement (form 103) to be included in the appropriate case file. The downloaded CD or other storage device will be subject to the same logging, handling, and chain of custody requirements as other evidence.
- F. Outside Agencies requesting access to information gathered by an ALPR will be directed to contact MCAC.
- G. If exigent circumstances exist or the incident presents a critical, time sensitive investigative request that come in from allied law enforcement agencies, the request can be approved by command staff. The Commander of the Detective Unit will be provided with a report of this action for audit and tracking purposes.
- H. The Duty Officer is responsible for entering all pertinent information related to an ALPR traffic stop and/or arrest in the Unit/Detachment's Daily Report.

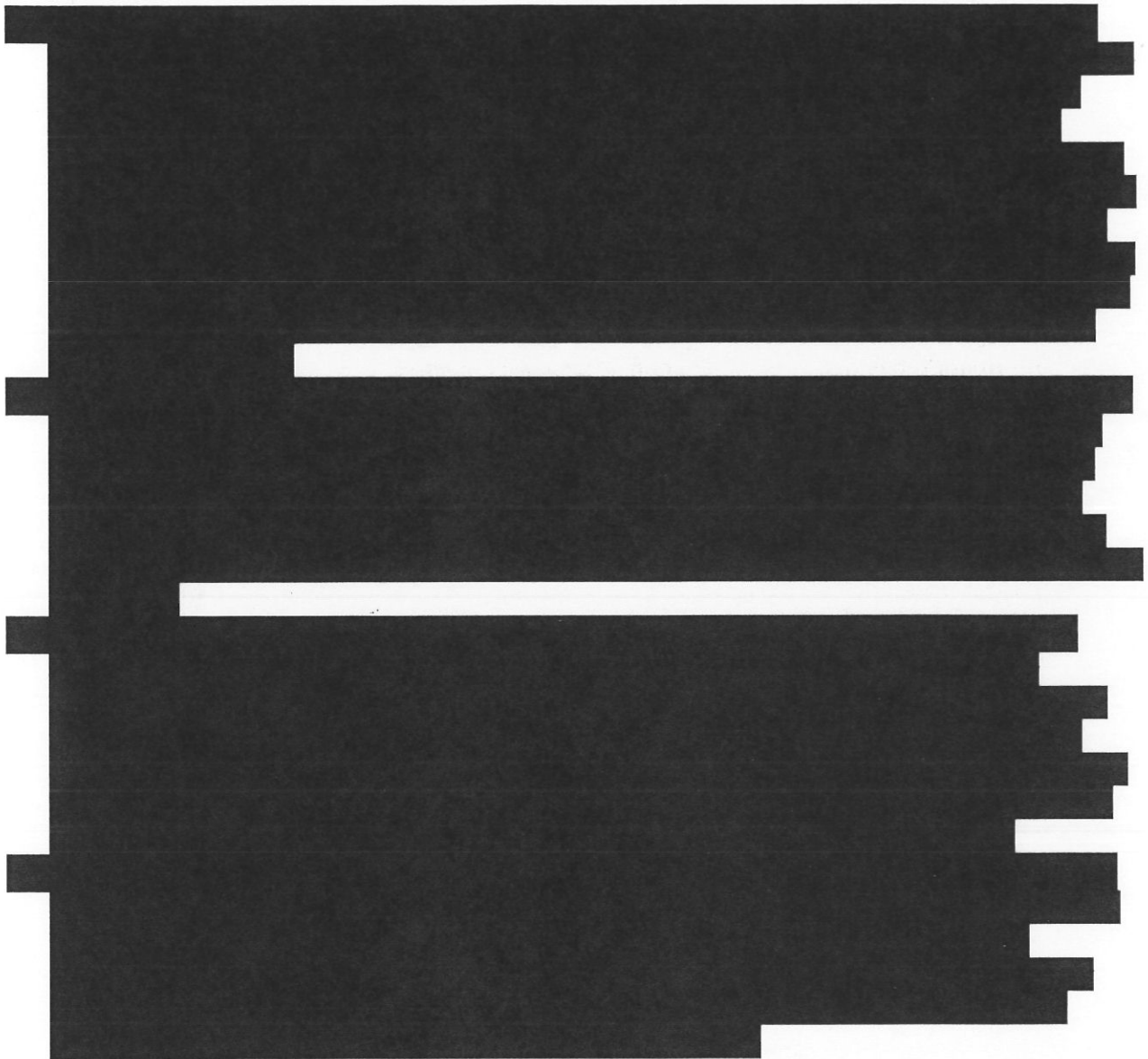
- I. Operators of ALPRs shall be responsible for keeping an accurate record of statistics to include: number of total reads, number of accepted alerts, number of rejected alerts and number of traffic/criminal enforcement actions taken. The unit/detachment commander is responsible to ensure that the mobile LPR data is entered weekly into the LPR database residing on the MDTA's "Shared" drive.

4. Operator Responsibilities

- A. ALPR operators shall be properly trained to operate the system. They are also responsible for proper maintenance and cleaning of the hardware.
- B. When an alert is accepted, Operators will confirm the information through METERS/CJIS. Absent other Probable Cause, ALPR operators will not initiate a traffic stop until the information has been verified. Upon a negative response, the Operator will reject the alert as it is no longer valid. If an alert is confirmed, the Operator will conduct a traffic stop in accordance with the appropriate MDTA policy.
- C. If an ALPR Operator has a confirmed "hit", but has lost the vehicle, the Operator should notify Communications as quickly as possible. Information relayed should contain: make and model of suspect vehicle, vehicle color, last known location, direction of travel and offense. Communications will then alert other Patrol Units in the area. If it becomes clear that the suspect vehicle will not be stopped before it leaves MDTA primary jurisdiction, Communications should notify other nearby agencies and relay all pertinent information.
- D. The highest priority for detection or notifying allied agencies should be given to Wanted Violent Criminals, AMBER, SILVER & BLUE alerts and other real time critical incidents.

5. Emergency Operations

- A. During the course of normal law enforcement duties, incidents may occur that require immediate attention. The ALPR system can be a valuable tool in these situations; such as bank robberies, AMBER, BLUE, and SILVER alerts or other violent crimes and can help bring the incident to a safe and successful conclusion. The data stored is also an excellent tool to assist with ongoing investigations.
- B. In the event of a critical situation with vehicle registration information, the deployment of the ALPR can maximize the coverage area to search for any vehicle involved.
- C. All license plate information related to a critical incident (i.e., AMBER, BLUE, and SILVER alerts, bank robbery suspect etc.) will be sent by MCAC, via a wireless connection, to ALPR units. If Communications announces a BOLO, it is the responsibility of the ALPR Operator to confirm that the MCAC "hotlist" reflects the updated information. If it doesn't, the ALPR Operator will manually enter the information into the system. Additionally, ALPR Operators will manually enter information for BOLOs that may be localized and not forwarded to MCAC for widespread distribution.
- D. When a tag is manually entered into the "hotlist", the system will automatically ask the user if they want a search of the database that will determine if the suspect vehicle has been recorded by the ALPR at an earlier time. Operators should click the "yes" button and inform the Duty Officer if any information is retrieved. The Duty Officer should immediately notify the jurisdiction issuing the request of any information retrieved.



E. All other Verified ALPR related traffic stop recording policies apply.

7. Chronic Toll Offenders (Scofflaws)

- A. A database has been created by the *E-ZPass*® office which contains the names and license plates of individuals who repeatedly use Authority facilities without paying the required tolls. These offenders have accrued unpaid tolls, fines and/or administrative charges. This database is updated as needed by an *E-ZPass*® representative. The database file will be added to a specified User Group at MCAC and uploaded to the ALPR system automatically via a wireless connection.
- B. The system will alert when one of these vehicles is recorded by a camera and will show “Scofflaw” as the offense.
- C. The Motor Vehicle Administration (MVA) has suspended the registrations of all scofflaw vehicles in the database.
- D. The procedure for “hit” confirmation is the same as with other alerts. Upon confirmation, the

patrol officer will proceed as with other suspended registrations. Violators will not be able to clear the registration suspension without settling their *E-ZPass*® account.

- E.** If personnel have questions about a Scofflaw account during regular Authority business hours, they can contact the *E-ZPass*® office at (410) 537-1393.

References

Police Directives Manual Chapter 16, Vendor Training Manual

Other Divisions Impacted

Patrol Division, Division of Operations, Division of Information Technology,

Contact Information

Information Technology Law Enforcement Unit

(410) 537-1350

Secondary information # (410) 537-1078

Procedure Status Information

This document can be found on MdTA Police Intranet

Original Date		Author	
05/10/11		Cpl. Eric Ferber	
Date of this revision:		Date of next revision: N/A	
Revision Number	Revision Date	Summary of Changes	Author
Approved by:		Title	Date
Antonio Rodriguez		Captain	08/09/11
Distributed to:		Title	

[Back to Top](#)

Attachments

Operator's Manual

**Standard Operating Procedures
License Plate Reader
Lane Memorial Bridge Detachment
(LPR)**

Version 2.4 Rev. 07/01/09

1. Definition

 The cameras send information via a network connection to a dedicated computer, which has been installed in the Communications room of the Bay Bridge Station.

2. Purpose

The system utilizes technology that matches the license plates of passing vehicles against a database of stolen vehicles, stolen registration plates, vehicles sought in connection with felony investigations and chronic toll evaders. The database can also include the information of vehicles wanted for other violations and will also support the purposes of Homeland Security.

3. System Deployment

The Detachment Commander, Assistant Commander, Shift Supervisor, or any of their Designees may suspend the use of the LPR at any time if necessary to maintain the proper running of the installation. The person suspending LPR operations is required to make an entry in the Detachment's Daily Report explaining why the action was taken, as well as noting how long the system was not being utilized.

4. Security Protocol

- A. Information in the Database is provided to the Police Department by CJIS via the Maryland Department of Public Safety. The information contained in the database is extremely sensitive. Everyone accessing the information will stay in compliance with all Federal and State Laws, as well as the MdTAP's Directives dealing with such information.
- B. The information is downloaded from the DPS secure website. The CJIS updates must be uploaded by 1200hrs on the day they are received. The TCO supervisor (or designee) will have the ability and authority to conduct the update. The information can be accessed by an authorized person on any agency computer that is connected to the internet. The information is never to be saved on a desktop or in any temporary file/folder. The information is only to be downloaded to a memory stick, which is dedicated to that one specific purpose. The information

on the memory stick will be uploaded on the LPR computer immediately after it is downloaded.

- C. The memory stick will be kept in a lockbox, which is mounted on the wall of the Communications room. The memory stick is only to be removed by authorized personnel. It should only be removed for the purpose of transferring data or other authorized reasons, and it will be removed from the lockbox at the time of use. The memory stick is to be returned to the lockbox as soon as the necessary work is completed.
- D. The Detachment Commander will have a key. An additional key will be kept in the Duty Office in a sealed envelope, accompanied by a logbook. Only a person authorized to access the information will be allowed to remove the key. The person removing the key will sign the logbook and fill in the appropriate spaces. The key is to be returned to the Duty Officer and re-sealed in a new envelope as soon as the necessary work is complete. The Duty Officer and the person using the key will sign the sealed envelope. The envelope will be returned to the cabinet where the other Detachment keys are stored.
- E. The system keeps a record of **all** vehicles that pass in front of the cameras for **180 days**. This information may become useful in later investigations. The Maryland Transportation Authority Police will only consider releasing information when the investigations involve matters of National Security or Part I Felonies. All requests from outside agencies must be in writing, and come from their Chief (or designee). Requests from Federal Agencies must come from the Agent in Charge (or designee). No information will be released without the **WRITTEN APPROVAL** of the MdTA Chief of Police or his designee. The Project Manager will oversee the processing of requests and the release of all information.
- F. The detachment commander (or designee) and the project manager shall have an account (username/password) which allows complete access to the system. This account will permit the entry of tag data, **database searches** and report generation. Each TCO and others designated by the detachment commander shall have an account which only allows the entry of tag data and system monitoring. The system can produce an audit report detailing the date, time and user related to all LPR activity.

5. TCO Responsibilities

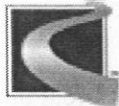
- A. The LPR system is located in the Communications room in close proximity to the Radio and the MILES/CJIS terminal. The TCO will be alerted by an audible tone when a vehicle matching the database passes in front of one of the cameras. The screen of the LPR computer will show all of the pertinent information to include; make and model, manufacture date, registration expiration, and reason the vehicle

is wanted. The LPR will also display a picture of the vehicle transmitted by the camera. This will allow the TCO to advise the patrol units of the color of the vehicle.

- B. When the system alerts the TCO of a suspect vehicle, the TCO will announce the following. "Bay Bridge to all units: attempt to locate the following LPR vehicle (followed by vehicle information). The TCO will provide the patrol units with all possible information. The LPR will display a real-time still photograph of the suspect vehicle [REDACTED] This will allow the TCO to pass other, more specific information to the patrol units.
- C. TCOs will always use the word "possible" when calling out an attempt to locate. TCOs will enter the information from the LPR into the MILES/CJIS terminal as soon as they call out the attempt to locate. **TCOs must alert the patrol units as soon as the information is verified through MILES/CJIS.** Just as in normal patrol procedures, the MILES/CJIS confirmation process will begin at the commencement of the traffic stop. Absent other Probable Cause, Patrol Units will not initiate a traffic stop until the information has been verified. Upon a negative response, the TCO will instruct the patrol units to disregard the attempt to locate. A positive response will direct the TCO to announce the vehicle information has been verified through the MILES/CJIS terminal.
- D. TCOs should announce the offense for which the vehicle is wanted. The announcement should be made as plainly as possible, with the TCO declaring the offense for which the vehicle is in the database (preceded by "Possible" until there is verification).
- E. TCOs will alert the Maryland State Police Centerville Barrack and the Queen Anne's County Sherriff's Department when it becomes apparent that MdTA patrol units will be unsuccessful in their attempt to locate. Patrol Units need to keep in mind the location of the vehicle when it is called out by the TCO [REDACTED] [REDACTED] If the responding Officer believes that he is out of position and unlikely to make visual contact with the suspect vehicle before it leaves our primary jurisdiction, he should notify communications so neighboring jurisdictions can be alerted.
- F. TCOs will document all LPR activity on the radio log as they would for any other radio transmission. The entry will include time of call out, vehicle information, result of search, and time allied agencies were alerted. Those entries should be highlighted in yellow. No CC Card is necessary unless warranted by a police action, per MdTAP policy.

6. Patrol Applications

- A.** Patrol Officers will acknowledge callouts for “attempt to locate” as soon as they are received. Officers should keep in mind that the TCOs are alerted when the vehicles are [REDACTED] Depending on the time of day, Officers will have a reasonable estimation when the suspect vehicle will exit the bridge on the Eastern Shore.
- B. Absent Exigent Circumstances, Officers are not to affect a traffic stop without Probable Cause until verification is received through CJIS/MILES.**
- C.** Upon verification Officers should take the appropriate action, either affecting a traffic stop consistent with the type of offense, or conducting the appropriate investigation to include proper reports and/or documentation per MdTAP policy.



Maryland
Transportation
Authority

Tunnel Command License Plate Reader

Document #:
Assigned by Budget &
Planning

Original
Approval Date:
06/16/10

Revised
Approval Date:

MDTA Police

Purpose Procedure References Other Divisions Impacted Contact Information Procedure Status DFD

Important Note: It is the responsibility of anyone using this SOP to ensure that he/she has the most current version.

Purpose

The purpose of this document is to outline the policies and procedures that govern the use of the License Plate Reader (LPR) at the Fort McHenry Tunnel. [REDACTED]

[REDACTED] A field control unit with a ruggedized brick PC is inside the TIF. The TIF requires proper ventilation and temperature control. The cameras send information via a network connection to dedicated computers, which are located in the Communications room of the Tunnel Command Detachment. The cameras capture the image of front and rear license plates.

The system uses technology that matches the license plates of passing vehicles against a database of stolen vehicles, stolen registration plates, vehicles sought in connection with felony investigations and chronic toll evaders. The database can also include the information of vehicles wanted for other violations (Amber, Silver & Blue alerts) and will also support the purposes of Homeland Security.

This document contains the following processes: System Deployment, Security Protocol, Data Collection, Retention & Dissemination, TCO Responsibilities, Emergency Operations, Patrol Applications and Terrorist/Gang Watch lists and Scofflaw Procedures.

Applicability:

This procedure is applicable to the MDTA Police, MDTA Police Communications and E-Z Pass® (scofflaw).

Responsibility:

LPR Administrator - (Detective Division Commander, ITLE Unit designee, Detachment Commander or designee) Responsibilities outlined in section 3.

Police Shift Supervisor – Responsibilities outlined in sections 3, 4 and 5.

TCO Supervisor - Responsibilities outlined in sections 2, 4 and 5. Ensure that all employees are made aware of this document and that they adhere to this SOP.

TCO – Responsibilities outlined in sections 4, 5 and 7.

Patrol Officer (Police) - Responsibilities outlined in sections 4, 5, 6, 7 and 8.

Detachment Commander - Ensure that all employees are made aware of this document and that they adhere to this SOP.

Equipment:

Fixed High Performance LPR Smart Camera and mounting hardware with all necessary electrical and communications connections ■■■, Field Control Unit with ruggedized brick PC, environmental controls, camera power supply, network switch and power conditioning, Operations Center Software and 2 desktop PCs, Hirschman Switches (1 per TIF)

1. System Deployment

The LPR is operational 24 hours a day. However, the Detachment Commander, Assistant Commander, Shift Supervisor, or any of their Designees may suspend the use of the LPR at any time if necessary to maintain the proper operation of the Detachment. The person suspending LPR operations must make an entry in the Detachment's Daily Report explaining why the action was taken, noting how long the system was not used.

2. Security Protocol

The NCIC information, known as the "hotlist" is automatically uploaded to the LPR twice daily (except Sundays and State Holidays) at 0700 and 1900. The TCO supervisor, or designee, shall confirm that the new list has been uploaded by: opening the "C" Drive on the LPR desktop, right clicking on the NCIC file, selecting "Properties" from the option list and verifying the "modified on" date. The modified date should reflect the current date and time updated. If the automatic download did not occur, the ITLE Unit (or their designee) will be notified.

3. Data Collection, Retention and Dissemination

- A. All system data collected by the Agency's LPR program will be maintained on the virtual machine server which is not accessible by any other law enforcement databases or personnel.
- B. Only trained personnel approved by an LPR Administrator may access system data on the server.
- C. Personnel are authorized/issued user names, passwords and access levels on an as needed basis as determined by an LPR Administrator (Detective Division Commander, ITLE Unit designee or Detachment Commander or designee). Accessibility levels determine if personnel can add tags to the LPR, conduct tag queries and/or run audit reports.
- D. All LPR system data downloaded to the server will be stored no longer than 90 days prior to purging unless it has become, or it is reasonable to believe that it will become, evidence in a specific criminal or civil action. Evidentiary value in a criminal case includes both evidence that will inculcate or exculpate a suspect.
- E. In those circumstances when data is identified as having evidentiary value, the Detective Division Commander (or designee) or Detachment Commander (or designee) specific to the incident will review the facts of the related case and determine if the data should be saved. If it is determined that the data has evidentiary value, the appropriate commander (or designee) specific to the incident will authorize the downloading of the applicable data from the server onto a CD or other portable storage device.
- F. This authorization will be documented on a Supplement (form 103) to be included in the

appropriate case file. The downloaded CD or other storage device will be subject to the same logging, handling, and chain of custody requirements as other evidence.

- G. The Commander and Assistant Commander of the Detective Unit will be given a username and password that will allow them to access the database and conduct searches in connection with MDTA Police investigations.
- H. The Maryland Transportation Authority Police will only consider releasing information to allied agencies when the investigation involves matters of national security or Part I Felonies. Allied agency requests to query LPR data must be submitted in writing on agency letterhead. The request must contain language that shows the requested information is for law enforcement purposes only in reference to a criminal investigation or national security matter. The Detective Unit Commander or his designee will provide the requesting agency with the information. These written requests shall be retained by the Detective Unit Administrative assistant for audit purposes for three years.
- I. If exigent circumstances exist or the incident presents a critical, time sensitive investigative request that come in from allied law enforcement agencies, the request can be approved by command staff. The Commander of the Detective Unit will be provided with a report of this action for audit and tracking purposes.
- J. The Duty Officer is responsible for entering all pertinent information related to an LPR traffic stop and/or arrest in the Tunnel Command Daily Report.

4. TCO Responsibilities

- A. The LPR system is located in the Communications room in close proximity to the Radio and the METERS/CJIS terminal. The TCO will be alerted by an audible tone when a vehicle matching the database passes in front of one of the cameras. The screen of the LPR computer will show all of the pertinent information to include; make and model, manufacture date, registration expiration, and reason the vehicle is wanted. The LPR will also display a picture of the vehicle transmitted by the camera. This will allow the TCO to advise the patrol units of the color of the vehicle.
- B. When the system alerts the TCO of a suspect vehicle, the TCO will announce the following over the radio: "Communications to all units: attempt to locate the following LPR vehicle (followed by vehicle information, direction of travel and suspected offense; **"Possible Stolen Vehicle"**). The TCO will provide the patrol units with all possible information. The LPR will display a real-time still photograph of the suspect vehicle [REDACTED] This will allow the TCO to pass other, more specific information to the patrol units.
- C. TCOs will always use the word **"possible"** when calling out an attempt to locate. TCOs will enter the information from the LPR into the METERS/CJIS terminal as soon as they call out the attempt to locate. **TCOs must alert the patrol units as soon as the information is verified through METERS/CJIS.** Just as in normal patrol procedures, the METERS/CJIS confirmation process will begin at the commencement of the traffic stop. Absent other Probable Cause, Patrol Units will not initiate a traffic stop until the information has been verified. Upon a negative response, the TCO will instruct the patrol units to disregard the attempt to locate. A positive response will direct the TCO to announce the vehicle information has been verified through the METERS/CJIS terminal. Patrol Units then have probable cause to initiate a traffic stop.
- D. TCOs should announce the offense for which the vehicle is wanted. The announcement should be made as plainly as possible, with the TCO declaring the offense for which the vehicle is in the database (preceded by "Possible" until there is verification).
- E. The highest priority for detection or notifying allied agencies should be given to Wanted Violent Criminals, AMBER, SILVER & BLUE alerts and other real time critical incidents.

When possible, TCOs will alert the Maryland State Police JFK Barrack, the Baltimore City Police (BPD), the Baltimore County PD, and any other appropriate Agency when it becomes apparent that MDTAP patrol units will be unsuccessful in their attempt to locate the suspect vehicle. Patrol Units need to keep in mind their location and travel direction of the vehicle when it is called out by the TCO.

- F. TCOs will document all LPR activity (verified alarms) in the "Verified LPR Log" that is kept near the LPR. The entry will include time of alert, bore and lane information, tag number, vehicle year, make and color, reason for the alert and result of search. No CC Card is necessary unless warranted by a police action, per MDTA Police (MDTAP) policy.

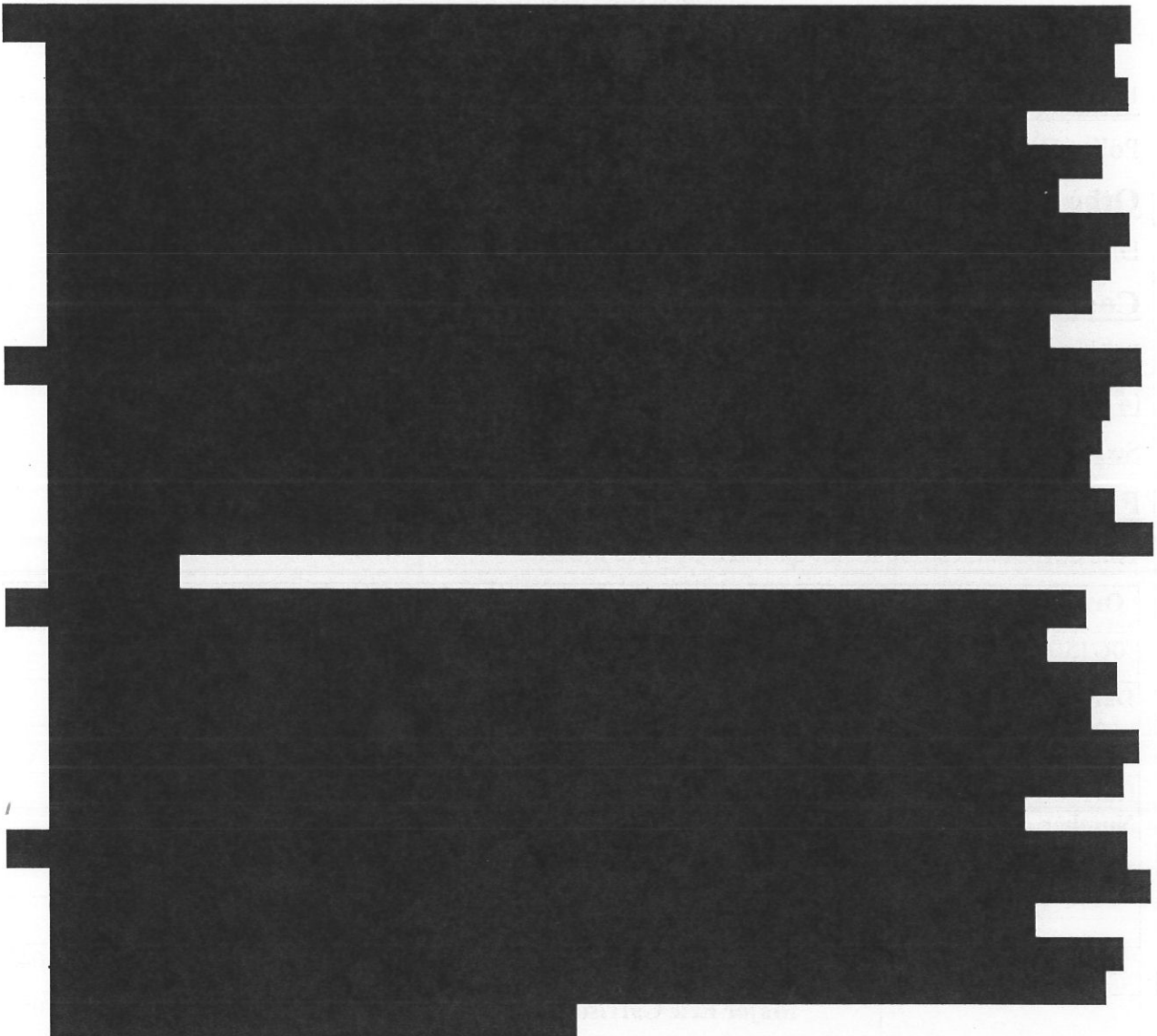
5. Emergency Operations

- A. During the course of normal law enforcement duties, incidents may occur that require immediate attention. The LPR system can be a valuable tool in these situations; such as bank robberies, AMBER, BLUE, and SILVER alerts or other violent crimes and can help bring the incident to a safe and successful conclusion. The data stored is also an excellent tool to assist with ongoing investigations.
- B. In the event of a critical situation with vehicle registration information, the deployment of the LPR can maximize the coverage area to search for any vehicle involved.
- C. All license plate information related to a critical incident (i.e., AMBER, BLUE, and SILVER alerts, bank robbery suspect etc.) will be immediately entered into LPR system by the LPR Administrator (Detective Division Commander) or designee (usually TCO) as soon as notification is received.
- D. Upon receiving notification that a critical situation requires manual entry of license plate information, the TCO must immediately review the details and notify the duty officer.
- E. Upon receipt of updated information, the TCO will immediately provide this information to the Duty Officer and Patrols. If an involved vehicle plate number changes, the TCO should make the necessary adjustment in the LPR system.
- F. When a tag is manually entered into the "hot list", the system will automatically ask the user if they want a search of the database that will determine if the suspect vehicle has been recorded by the LPR at an earlier time. Personnel should click the "yes" button and inform the Duty Officer if any information is retrieved. The Duty Officer should immediately notify the jurisdiction issuing the request of any information retrieved.

6. Patrol Applications

- A. Patrol Officers will acknowledge callouts for "attempt to locate" as soon as they are received. Officers should keep in mind that the TCOs are alerted when the vehicles [REDACTED] [REDACTED] Depending on the time of day, Officers will have a reasonable estimation when the suspect vehicle [REDACTED].
- B. **Absent Exigent Circumstances, Officers are not to make a traffic stop without Probable Cause until verification is received through METERS/CJIS.**
- C. Upon verification Officers should take the appropriate action, either affecting a traffic stop consistent with the type of offense, or conducting the appropriate investigation to include proper reports and/or documentation per MDTAP policy.

7. [REDACTED]



E. All other Verified LPR call-out and LPR related traffic stop recording policies apply.

8. Chronic Toll Offenders (Scofflaws)

- A. A database has been created by the *E-ZPass*® office which contains the names and license plates of individuals who repeatedly use Authority facilities without paying the required tolls. These offenders have accrued unpaid tolls, fines and/or administrative charges. This database is updated as needed by an *E-ZPass*® representative. The database file will be added to a specified folder on the S Drive and uploaded by the LPR system automatically.
- B. The system will alert when one of these vehicles is recorded by a camera and will show "Scofflaw" as the offense.
- C. The Motor Vehicle Administration (MVA) has suspended the registrations of all scofflaw vehicles in the database.
- D. The procedure for "hit" confirmation is the same as with other alerts. Upon confirmation, the patrol officer will proceed as with other suspended registrations. Violators will not be able to clear the registration suspension without settling their *E-ZPass*® account.

E. If personnel have questions about a Scofflaw account during regular Authority business hours, they can contact the *E-ZPass*® office at (410) 537-1393.

References

Police Directives Manual Chapter 16, Vendor Training Manual

Other Divisions Impacted

Division of Operations, Division of Information Technology, Division of Engineering

Contact Information

Information Technology Law Enforcement Unit

(410) 537-1350

Secondary information # (410) 537-1078

Procedure Status Information

This document can be found on MdTA Police Intranet

Original Date		Author	
06/15/10		Cpl. Eric Ferber	
Date of this revision: 07/21/10		Date of next revision: N/A	
Revision Number	Revision Date	Summary of Changes	Author
1	07/21/10	Changes to the following categories: Responsibilities, Section 1, Section 3 and Section 8.	Cpl Eric Ferber
Approved by:		Title: Captain Antonio Rodriguez	Date 05/04/11
		Major Eric Garrison	05/05/11
Distributed to:		Title: All MDTA Police	

[Back to Top](#)

Data Flow Diagram

See Attached



Ft. McHenry Tunnel LPR Setup

- 1. Data** – Multiple source data can be combined
 - NCIC national stolen vehicle and plate data published daily by the FBI
 - Includes stolen vehicles, plates, wanted people
 - EZ Pass toll violator data is also included
 - MVA Data is available and may one day be included
 - BOLO PLATES can be added at any time.
- 2. Setup** – Two monitors in Communications Center, marked Northbound and Southbound
 - 8 NORTHBOUND CAMERAS, 2 FRONT AND 2 REAR PER BORE
 - 8 SOUTHBOUND CAMERAS, 2 FRONT AND 2 REAR PER BORE
 - EACH CAMERA IS LABELED BY ITS LANE
 - CAMERAS ARE LOCATED ON LAST GANTRY BEFORE TUNNEL ENTRY
- 3. Monitors are for viewing:** Hotlist changes and data queries happen at the ELSAG Operations Center on the Desktop
- 4. Is it Running?** – System is operational if LPR Light at bottom of screen is green and you are seeing photos of cars constantly changing.

The Challenge of U.S. Plates

□ All License Plates are NOT Created Equal

□ The Magic is in the Details that Can Make All the Difference in Results

□ High performance levels of the OCR algorithms achieved through customization — 95%+ accuracy

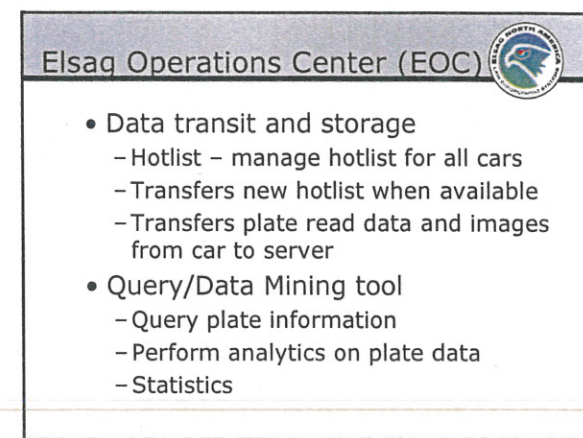
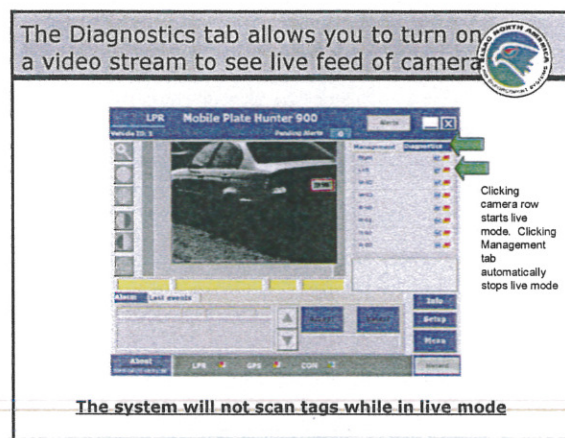
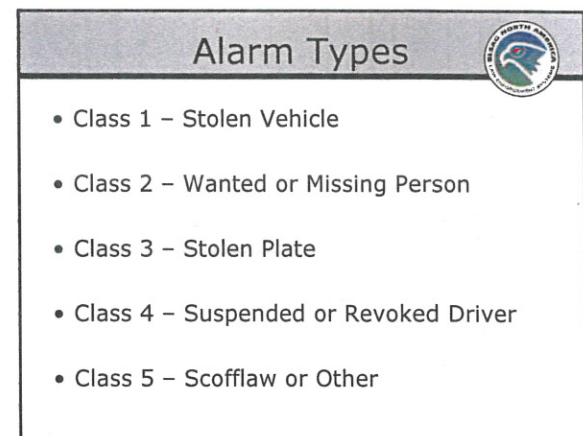
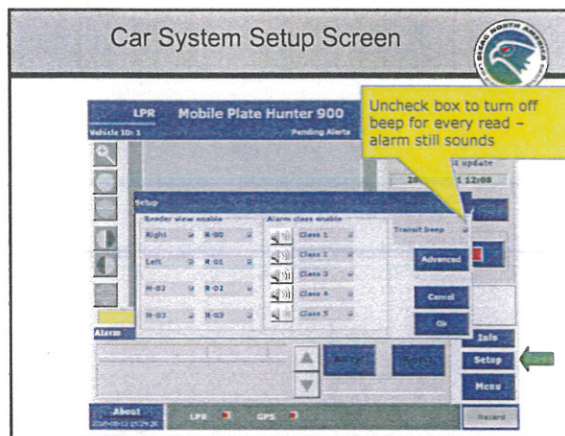
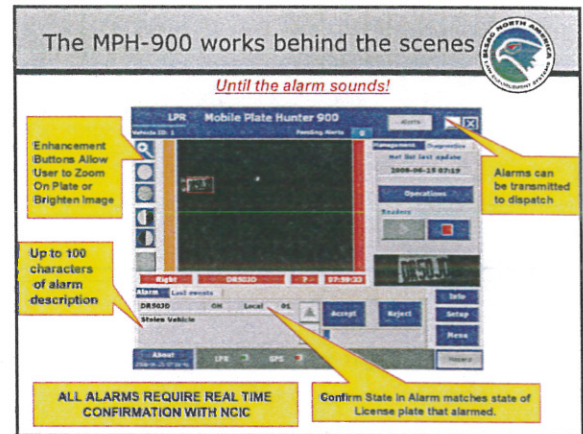
□ Only LPR Provider that can read plates in all 50 states including Canada and Mexico

Camera Range and Performance

- Operates at 140 MPH passing and closing speeds
- Works day or night, in any kind of weather
- Cameras capable of reading 900 plates per minute
- Reads plates from all 50 states including flat and red character plates
- Performs ambiguous searches to improve accuracy
- Alerts within milliseconds if a vehicle is suspect
- Multi-level alarm levels for prioritization
- Can be configured with a variety of different camera ranges
- Can be configured to remotely alarm to an email recipient
- Can operate with data from different sources and be updated on the fly

Car System Menu Screen

Main Car System Screen



Operations Center

http://.../Operational_Center (shortcut on Desktop)
User: systemadmin Password: systemadmin

Dashboard

- Overview of data transfer status between server and cars
- Hotlist – Completed, Aborted, Failed
 - Date and time of last transfer
 - Last file on Car
- Images – Completed, Aborted, Failed
 - N. files to transfer – number of files on the car that need to go to server
 - N. transferred files – how many files actually made it to server
- Reads – Completed, Aborted, Failed

Dashboard

- Import Status
 - Filename has date in it
 - All three phases should be 100%
- Statistics
 - For last day only

Statistics

- To display statistics, simply choose a start and end date

Statistics

Statistics

Query Page

- Query plate read data
 - Time and Date
 - Full or Partial Plate
 - Per car
 - Per Alarm Type and/or Class
 - Via map
 - Via Location Radius

Query

- Step 1 choose a start and end date and time

Start Date:
 End Date:
- Step 2 (optional) choose a full or partial plate and/or state

License Plate: State:
- Step 3 (optional) choose a car or transit type. If nothing is selected all cars and transit types are included. If alarm type is chosen further filtering via Alarm Class is possible.

Car#1
Car#2
Car#3
Car#4
Car#5
Car#6
Car#7
Car#8
Car#9
Car#10
Car#11
Car#12
Car#13
Car#14
Car#15
Car#16
Car#17
Car#18
Car#19
Car#20
Car#21
Car#22
Car#23
Car#24
Car#25
Car#26
Car#27
Car#28
Car#29
Car#30
Car#31
Car#32
Car#33
Car#34
Car#35
Car#36
Car#37
Car#38
Car#39
Car#40
Car#41
Car#42
Car#43
Car#44
Car#45
Car#46
Car#47
Car#48
Car#49
Car#50
Car#51
Car#52
Car#53
Car#54
Car#55
Car#56
Car#57
Car#58
Car#59
Car#60
Car#61
Car#62
Car#63
Car#64
Car#65
Car#66
Car#67
Car#68
Car#69
Car#70
Car#71
Car#72
Car#73
Car#74
Car#75
Car#76
Car#77
Car#78
Car#79
Car#80
Car#81
Car#82
Car#83
Car#84
Car#85
Car#86
Car#87
Car#88
Car#89
Car#90
Car#91
Car#92
Car#93
Car#94
Car#95
Car#96
Car#97
Car#98
Car#99
Car#100

Transit status
☐ Car
☐ Transit
☐ Both

Alarm Class
☐ Car
☐ Transit
☐ Both

Advanced Query

- Partial Plate wildcard characters
 - % around known characters for general wildcard
 - @ Letter specific wildcard
 - # Number specific wildcard
- D% - Every plate that starts with D
- %D% - Every plate that has D in the middle
- %D - Every plate that ends in D
- D@@#### - Every plate that starts with D where the next two characters are letters and the next four are numbers.

Data Mining

- Cross Search
 - Analyze plate data from two separate time frames
 - Show unique plates in each time frame
 - Show duplicates in both time frames
 - Great for arson, burglary, assault investigations

Cross Search

Step 1 – Choose the first time period using standard query tools

Cross Search

Step 2 – Choose the second time period using standard query tools

Cross Search

Step 3 – Choose "Unique in first", "Unique in second", or "Duplicates"

Nested and Convoy

Click on License Plate hyperlink to see all instances of that plate read

License Plate	State	Time	Location	Status	Type	Count
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1

Nested and Convoy

- Click on car icon to perform convoy analysis
- Display 15 car in front of and 15 cars behind the base car.
- Developed for the DEA.

License Plate	State	Time	Location	Status	Type	Count
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1
2450A 2009 214213	MD	11/11/2009 16:42:13	Normal Transit	MD	Normal Transit	1

Hotlist Management



Automated: Hotlist ready to be imported

Wait please...

- Insert/Delete Plate for BOLO...

Import Plate List Import/Delete PL

License Plate: State:

Notes: Alarm Class:

Insert Hot List

Hotlist Management



- Show plates in hotlist

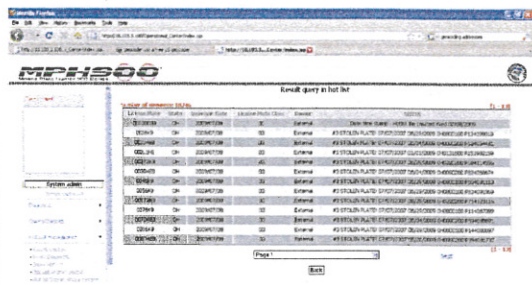


Plate	State	Alarm Class	Alarm	Alarm Date	Alarm Time	Alarm Status
12345678	NC	01	ALARM	2007-01-01	10:00:00	Active
87654321	NC	02	ALARM	2007-01-01	10:00:00	Active
98765432	NC	03	ALARM	2007-01-01	10:00:00	Active
10987654	NC	04	ALARM	2007-01-01	10:00:00	Active
21098765	NC	05	ALARM	2007-01-01	10:00:00	Active
32109876	NC	06	ALARM	2007-01-01	10:00:00	Active
43210987	NC	07	ALARM	2007-01-01	10:00:00	Active
54321098	NC	08	ALARM	2007-01-01	10:00:00	Active
65432109	NC	09	ALARM	2007-01-01	10:00:00	Active
76543210	NC	10	ALARM	2007-01-01	10:00:00	Active

Server Management



- Emails for alarm notification
- Configurable based on alarm class

Add new Email Address New By

Email Alarm Class

☐ 00 ☐ 01 ☐ 02 ☐ 03 ☐ 04 ☐ 05 ☐ 06 ☐ 07 ☐ 08 ☐ 09 ☐ 10

Save

Contact Info



Toll Free Support #:
1-866-967-4900

Contact Name: Jason Laquatra
Cell: 336-453-4516

Contact Name: Greg Lewis
Cell: 301-509-5736

Chapter 8 – Police Records



3

Directives Manual Revision Date: 12-01-11

6.2 Shift Supervisors and/or Duty Officers are authorized to access files and records during hours when the Detachment's records are closed to the public, thus providing 24-hour access to operations personnel. A key shall be readily available in the supervisor's office at all times.

7. Report Accounting System

7.1 The MdTA Police Central Records will maintain the original of all reports along with follow-up reports under the original complaint control number.

7.2 Once a report has been assigned to an officer for follow-up investigation, all additional information will be documented via Supplement/Continuation Report(s) in accordance with the Field Reporting Manual.

7.3 All supplemental reports will follow a specified schedule in accordance with the Case File Management procedures, as detailed in Chapter 26.

8. Annual Audit of Central Records Computer

8.1 An annual audit will be conducted of the Central Records computer system for verification of all passwords, access codes, or access violations according to State Computerized Record System Security Requirements, Section IV. C. 6-7.

8.2 It will be necessary for the Administrative Services Bureau Chief to contact Division of Information Technology (DoIT) requesting the audit information for Central Records.

9. Software Policy

9.1 A written directive has been established for the introduction of outside computer software and disks into agency-owned computer systems to avoid a virus infection of the host system in accordance with the State Computerized Record System Security Requirements, Section IV. A. 10.

9.2 All disks or software are to be inspected by DoIT personnel prior to introduction to the agency-owned computer system. The agency shall ensure that the software is properly licensed in accordance with State Computerized Record System Security Requirements, Section IV. A. 10.

10. Computer File Backup and Storage

10.1 Computer files shall be backed up on a daily basis and comply with the agency retention schedule which conforms to record retention laws and regulations.

10.2 All tapes, disks or drives shall be stored off-site in a secure area in accordance with State Computerized Record System Security Requirements, Section IV. A. 5-6.

10.3 Any tapes, disks or drives that are not recycled shall ensure that data is not retrievable from the discarded source in accordance with State Computerized Record System Security Requirements, Section IV. B. 5.

11. Computerized Security Protocol

11.1 Criminal history record forms are kept in a secured file. The form provides for dissemination of records. Access is limited to authorized Telecommunications and Police personnel.

12. Master Name Index

12.1 The MdTA Police will maintain a master name index that serves as a cross-reference to reports in which a person has been named in its computer system.

12.2 Names listed in the master name index file include victims, complainants, suspects, and arrested persons.

12.3 A separate master name index file will be maintained on persons involved in traffic accidents.

12.4 The MdTAP's computer system stores records, which include crimes by type, crimes by location, and stolen, found, recovered and evidentiary property files

13. Traffic Records System

13.1 The primary goal of the MdTA Police traffic records system is to reduce the number of motor vehicle collisions in the jurisdictions of the MdTA Police. Valid collision and enforcement data will be made available to provide the Patrol Division Commander, Special Operations Division Commander, Chief of Police, and other highway safety related groups with useful, adequate and timely information on which to base collision prevention efforts and preventive programs. The traffic records system shall contain information on all collisions and traffic enforcement measures taken within the Maryland Transportation Authority jurisdiction.

13.2 The MdTA Police traffic records system includes the following:

Chapter 8 – Police Records



7

Directives Manual Revision Date: 12-01-11

Section III - Auxiliary Personnel Files

1. Policy

1.1 It is the policy of the Maryland Transportation Authority Police to maintain Auxiliary Personnel files at the detachment or unit level in accordance with State Government Article, Title 10 of the Annotated Code of Maryland and related federal regulations.

1.2 Auxiliary Personnel Files consists of personnel related records kept at the detachment level for each sworn employee. This will enable the Commander and supervisors to maintain and readily access appropriate information related to each sworn member of the unit.

1.3 MdTA Human Resources will maintain the Permanent Personnel Folder and all medical related information. Copies of medical related information will not be filed in auxiliary personnel file but filed separately.

1.4 The Internal Affairs Unit will maintain all records involving disciplinary action and complaints. Copies of suspensions or loss of leave will be filed in Auxiliary Personnel File section 1-17, Job Performance Documentation.

1.5 Auxiliary Personnel Files will be maintained for the duration of an employee's tenure with the Maryland transportation Authority Police. The Auxiliary Personnel File accompanies the employee when transferred.

1.6 When sworn employees separate from the MdTAP, Commanders will forward the entire Auxiliary Personnel File to the Human Resources Coordinator. The Human Resources Coordinator will merge the Auxiliary and Permanent Personnel File and retain per policy.

1.7 As a general rule, copies of the documents should be contained in the Auxiliary Personnel Files. The originals should be maintained in the Permanent Personnel folder.

2. File Maintenance

2.1 Commanders or their designees will maintain the Auxiliary Personnel Files under lock-and-key in a secure location.

2.2 Files maintained for each sworn employee assigned to the detachment or unit will be arranged alphabetically in one location.

2.3. Letter size manila folders will be used for file subdivisions. Commanders may use hanging folders or

accordion folders to maintain the Auxiliary Personnel File for each employee.

3. Filing System & Retention Schedules

3.1 The retention schedule and file set up for all categories of auxiliary files will be maintained on the Police Manuals page of the intranet.

Chapter 16 – Patrol



17

Directives Manual Revision Date: 04/23/12

Section VII – License Plate Reader (LPR)¹⁸

1. Objectives

1.1 License plate readers will be used for the following purposes:

- Identify persons wanted for homeland security investigations
- Identify and recover stolen vehicles and plates
- Identify and recover vehicles wanted in Amber, Blue, and Silver Alerts
- Identify and recover vehicles operating with suspended registrations
- Identify vehicles whose owners' license is suspended
- Identify chronic toll offenders (scofflaws)

2. Operation

2.1 License plate readers shall only be operated by personnel that have been trained in their use. Operators shall only use the LPR in accordance with their training.

2.2 Each person assigned an LPR is responsible for the care of the equipment. LPR equipment shall be cleaned and maintained according to the manufacturer's recommendations.

2.3 Shift supervisors may suspend the use of a fixed LPR at any time. An entry explaining the suspension must be made in the detachment's Daily Report.

2.4 The Lead LPR Coordinator shall prepare and maintain Standard Operating Procedures for both fixed and mobile LPRs.

2.5 Personnel that receive an alert of a positive hit on a scanned license plate will compare the digital image of the license plate to the NCIC information to verify the hit.

2.6 An alert does not constitute probable cause. Traffic stops will not be initiated until verification is received through CJIS/MILES or other probable cause is developed.

3. Emergency Operations

3.1 TCOs shall notify the shift supervisor of all Amber, Blue, and Silver alerts and Part 1 Crime lookouts. All license plate information will be passed to mobile LPR users who shall immediately enter the information into the mobile LPR. TCOs shall enter the information into the fixed LPR.

3.2 Upon receipt of updated information, TCOs shall immediately notify the shift supervisor and patrols and enter the update into the fixed LPR.

3.3 All LPR users shall immediately search the LPR vehicle databases to determine if a record of past encounters exists.

4. Fixed LPR Security

4.1 Automated CJIS updates to the LPR hotlist will occur at 0700 and 1900 daily. The means by which the updates are downloaded shall be kept secure at all times.

4.2 Detachment commanders, their designees, and the Lead LPR Coordinator shall have an account that allows complete access to the LPR system. Each TCO and others designated by the detachment commander shall have an account that allows system monitoring and entry of tag data.

5. Mobile LPR Security

5.1 Mobile LPR operators shall ensure that the LPR system and all associated equipment are kept secure from unauthorized access.

6.1 Records

6.1 TCOs will document all LPR activity on the radio log. The entry will include the time of call out, vehicle information, result of the search, and time allied agencies were notified. The entries should be highlighted in yellow. A CC card is necessary only if police action occurs.

6.2 Each Detachment/Unit assigned LPRs, whether mobile or stationary, will report the following information (alerts accepted, verified alarms, probable cause stops, and law enforcement actions) weekly

- Number of stolen vehicles
- Number of chronic toll violators (Scofflaws)
- Number of vehicles with suspended operators
- Number of vehicles under Amber Alert
- Silver Alerts
- Number of vehicles with suspended registrations
- Number of stolen plates
- Number of vehicles with wanted persons
- Number of vehicles with persons subject to protective orders
- Terrorists, Gangs, and other Persons of Interest
- Missing persons located

Chapter 16 – Patrol



18

Directives Manual Revision Date: 04/23/12

- All other Alerts

6.2.1 This information will be entered by each detachment/unit into the Police License Plate Reader Database on the shared drive.

6.3 Upon approval of a commander, a sworn member of the MDTA Police may release information captured by LPR's to other law enforcement agencies upon the receipt of a written request. LPR data may only be released for official law enforcement use.

6.4 All written requests to review stored data shall be forwarded to the Commander of the Budget & Planning Command by the commander who approved the request. This documentation will be physically stored or stored electronically for three years.

6.5 All LPR data will be stored until it is uploaded to the State repository at the Maryland Coordination and Analysis Center.

6.6 All data gathered with an LPR is for official use only.

7. Audit

7.1 The Staff Inspection Section of the Budget & Planning Command shall conduct periodic audits of LPR records to deter and discourage misuse of the system. The results of the audit will be passed directly to the Commander of the Budget and Planning Command. The Commander of the Budget and Planning Command shall notify the Internal Affairs Unit of suspected misuse.

Maryland Transportation Authority Police LPR Data
FY 2012

Month	July	Aug.	Sept.	Oct.	Nov.	Dec.	Jan.	Feb.	Mar.	Apr.	May	June
LPR Reads	3,227,973	8,558,959	8,558,959	5,933,163	4,641,836	3,699,518	3,426,223	2,017,999	2,921,402	0	3,429,076	1,288,769
Accepted Alarms	533	851	867	382	760	781	227	756	296	0	291	188

LPR Data was lost for April 2012 due to this S Drive crash. Data could not be recovered.

Fixed LPR Unit at Tunnel Command was taken off line in June due to CDC construction.