



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

October 8, 2013

Dear Chief:

Attached, please find two documents concerning the use of Automatic License Plate Reader (ALPR) technology. The first document is the *Commonwealth Criminal Justice Information Services Automatic License Plate Recognition Systems Central Repository Companion Policy*. This is the policy that governs the statewide centralized data warehouse that stores ALPR information contributed by law enforcement and public safety agencies. The second document is a model policy for law enforcement agencies concerning the use of ALPR systems. Many departments requested that the Executive Office of Public Safety and Security (EOPSS) provide a model ALPR policy that they may consider adopting in their jurisdiction.

ALPR technology is an effective mechanism to increase public safety by enhancing existing law enforcement capabilities. Capable of recognizing over 1,000 license plates an hour on vehicles as they pass either a portable or stationary unit, an ALPR system reads a plate, compares it against a locally stored list of plates known as a CJIS-NCIC Hotfile database (“Hotfile”) and alerts the officer to any matches. The Hotfile consists of license plate numbers associated with suspended and revoked licenses, stolen vehicles, AMBER Alerts, Missing Child Alerts, Missing College Student Bulletins, and Be On Look Out (BOLO), Attempt to Locate (ATL), or Wanted or Missing Person broadcasts or bulletins in which a license plate number is included.

The Hotfile 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) or Department of Homeland Security watch lists. The Registry of Motor Vehicles can provide lists of expired registration tags, and law enforcement agencies can interface their own, locally compiled hot lists to the ALPR system. In addition to agency supported hot lists, users may also manually add license plate numbers to hot lists in order to be alerted if and when a vehicle license plate of interest is “read” by the ALPR system. When a targeted plate is located, the officer is notified with a visual or audio alert. ALPR systems record every license plate viewed, as well as the location, date and time of each license plate read.





ALPR data can be electronically submitted to the state central repository maintained by the Department of Criminal Justice Information Services (DCJIS). Departments that procured ALPR systems through a grant from EOPSS have agreed, as a condition of acceptance of grant funds, to electronically submit their captured ALPR data to the state central repository. The DCJIS central repository policy and model department policy were crafted recognizing the importance of balancing law enforcement goals with potential privacy concerns. Since the use of ALPR technology must be consistent with the high standard of privacy protection under Article 14 of the Massachusetts Declaration of Rights, the policies include privacy safeguards which not only restrict data access, but also secure the data and provide for audit functions to ensure compliance with the policies.

I hope you will find these documents useful for your department.

Very truly yours,

A handwritten signature in black ink that reads 'James F. Slater III'. The signature is written in a cursive style with a large, looping initial 'J'.

James F. Slater, III
Acting Commissioner

cc: Anne P. Powers, Undersecretary for Law Enforcement
Curtis M Wood, Undersecretary for Forensic Science and Technology
Major Dermot Quinn, Massachusetts State Police



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.



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.

**MASSACHUSETTS DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES
GLOBAL JUSTICE AND PUBLIC SAFETY USER AGREEMENT**

1.0 Purpose

This Global Justice and Public Safety User Agreement (hereinafter, "Agreement") establishes guidelines for the access, use, dissemination, and sharing of criminal justice information (CJI) collected and maintained within the systems and networks operated, maintained, and managed by the Massachusetts Department of Criminal Justice Information Services (DCJIS).

2.0 Authority

This Agreement is established pursuant to M.G.L. c. 6, s. 167-1788, M.G.L. c. 6, s. 18 %, 803 CMR 7.00, and 28 C.F.R. Part 20.

3.0 Scope

This Agreement is applicable to all sworn and non-sworn employees, contractors, interns, volunteers, and information technology support staff of all criminal justice and public safety agencies in the Commonwealth of Massachusetts who utilize or otherwise have access to any software application, system, network, or CJI operated, maintained, or managed by the DCJIS

4.0 Duration of Agreement

This Agreement is in effect until modified or cancelled by the DCJIS. Each Agency Head shall sign off on a copy of this Agreement as a condition of access to the systems and networks operated, maintained, or managed by the DCJIS. In addition, each Agency Head will sign off on a copy of the Companion System Agreement for EACH system for which such an agreement exists. An original, signed copy of this Agreement, along with original, signed copies of any Companion System Agreements, will be kept on file at the DCJIS. The Agency Head shall maintain a copy of the signed agreements. Facsimile and electronic signatures are acceptable as originals.

The Agency Head also agrees to execute a new Global Justice and Public Safety User Agreement and all relevant Companion System Agreements in accordance with 803 CMR 7.06 whenever there are changes to the Agency Head, the CJIS Representative, the backup CJIS Representative, or the CJIS Technical Representative. The new Agreement(s) is/are to be executed within ten (10) business days of the effective date of the change(s) necessitating a new Agreement(s). Original, signed copies of the newly executed Agreement(s) will be forwarded to the DCJIS within ten (10) days of execution.

5.0 Definitions

Authorized User

A sworn or non-sworn justice or public safety employee, contractor, intern, volunteer, or IT support staff member who has been authorized by his/her agency head to access any software application, system, network, or CJI operated, maintained, or managed by the DCJIS

Companion System Agreement

An addendum or "rider" to this Agreement. Each Companion System Agreement establishes rules and protocols for contributing CJI to, or accessing, using, or disseminating CJI from, a specific system or database operated, maintained, or managed by the DCJIS.

Criminal Intelligence System

A system that stores detailed intelligence or investigative information on the suspected criminal activities of subjects and/or which stores only information designed to identify individuals or organizations that are the subject of an inquiry or analysis.

Criminal Justice Information (CJI)

CJI is defined as all data obtained from or through the CJIS necessary for law enforcement and civil agencies to perform their missions. CJI includes, but is not limited to, biometric, identity history, biographic, property, and case/incident history data.

Criminal Justice Information System (CJIS) Representative

The CJIS Representative serves as the primary agency point of contact for the DCJIS. Responsibilities include ensuring that all DCJIS system usage and security policies and procedures are being followed by the agency, training all agency personnel who access any system or network operated, maintained, or managed by the DCJIS or who use the CJI obtained from or through those systems and networks, and attending all DCJIS-sponsored meetings, seminars, and conferences.

Criminal Justice Information System (CJIS) Backup Representative

The Backup CJIS Representative shall be the DCJIS' secondary point of contact for the agency. The Backup CJIS Representative shall assume all of the duties and responsibilities of the CJIS Representative should the CJIS Representative be unable to perform those duties and responsibilities for any reason.

Criminal Justice Information System (CJIS) Technical Representative

The CJIS Technical Representative serves as the primary agency point of contact for the DCJIS on all technology-related matters. The Technical Representative's main responsibility is to ensure that the agency meets the requirements of the FBI CJIS

Security Policy. The CJIS Technical Representative may also serve as either the CJIS Representative or the Backup CJIS Representative.

Criminal Justice Information System (CJIS) User-Access Model

A single-identity management model used to authenticate users of the software applications, systems, and networks operated, maintained, or managed by the DCJIS.

Justice and Public Safety Enterprise Application

A software application which criminal justice and public safety agencies use to contribute CJI to, or to access CJI from, databases or systems maintained by or accessed through the DCJIS.

Non-Contributing Agency

An agency that may access CJI from, but which does not contribute CJI to, a database or system operated, maintained, or managed by the DCJIS.

Source Agency

The agency that originally recorded and contributed data to a database or system operated, maintained, or managed by the DCJIS.

6.0 DCJIS Transaction Logs

An audit log of all transactions made by CJIS user agencies is maintained by the DCJIS. This log records the identity of the individual user and agency accessing the system, the date and time of access, and the data entered into, or retrieved from, any database or system operated, maintained, or managed by the DCJIS.

An Agency Head may request a report of all transactions initiated by the users of his/her agency. All report requests must be submitted in writing to the DCJIS.

The DCJIS CSO, at his/her discretion, may, at any time, authorize additional audits of all databases and systems operated, maintained, or managed by the DCJIS.

7.0 Audits of CJI Users

The DCJIS will conduct audits of all agencies, both criminal justice/public safety and non-criminal justice, accessing or using the CJI stored within, or obtained through, the databases, systems, and networks operated, maintained, or managed by the DCJIS. The purpose of these audits is to ensure the integrity and security of the CJI, applications, and systems, to investigate potential inappropriate use of these resources, and to identify potential training needs.

Each CJIS user agencies will be audited at least on a triennial basis (once every 3 years).

8.0 Justice and Public Safety CJI System and Network Usage Restrictions

Use of any CJI obtained from or through an application, database, system, or network operated, maintained, or managed by the DCJIS is limited to legitimate justice and public safety purposes within the scope of a user's employment and official duties. OCJIS resources may not be used for personal gain or for personal use, or to assist another individual or entity that is not authorized to access, use, or receive CJI from these resources. Criminal intelligence systems may also be subject to 28 CFR Part 23. Where the provisions of this Agreement or its addenda conflict with 28 CFR Part 23, 28 CFR Part 23 shall supersede this Agreement and its addenda.

9.0 Misuse

An Agency Head is responsible for investigating all alleged incidents or allegations of misuse of any CJI or database, system, or network operated, maintained, or managed by the DCJIS. If an Agency Head determines that someone within his/her agency has misused any of these resources, he/she must, within 10 business days, notify the DCJIS CSO in writing of the circumstances surrounding the misuse, of the actions taken, or to be taken, to address and correct the misuse, and of the policy(ies) and procedures to be implemented to prevent future misuse. The DCJIS CSO may suspend or revoke access to any or all databases or systems operated, maintained, or managed by the DCJIS for the individual(s) involved in the misuse.

Misuse of any DCJIS-provided CJI or resource may result in individual loss of access to the resources, agency loss of access to the resources, and/or state and federal civil and criminal penalties, if applicable. Users are also subject to the rules and regulations of their respective agency.

10.0 Access to DCJIS Resources

Sworn and non-sworn justice and public safety employees, as well as the employees of non-criminal justice agencies, may be granted access to one or more DCJIS applications, systems, and networks as authorized by the Agency head.

Each individual accessing a OCJIS resource will be assigned a unique user identifier (User ID) and initial password. The individual will be required to change his/her password when logging into a resource for the first time. When possible, the same User ID and Password will enable a user to access multiple OCJIS resources. However, some applications may require a separate log in and/or a different User ID and Password.

All passwords used to access a OCJIS resource will meet the OCJIS and FBI security requirements in effect at the time the password is created/changed.

Authorized users shall not share their passwords and user identifications with any other individual. Each authorized user shall be responsible for all transactions conducted with his or her user identification and password.

Agencies are responsible for notifying the DCJIS, in writing, when a user is no longer authorized to access DCJIS resources. DCJIS will terminate or suspend user access depending on the user's status within his/her respective agency.

User IDs and passwords shall be reviewed by each agency on an annual basis. The Agency Head and agency CJIS Representative shall be responsible for this review. The purpose of this review is to confirm the continued authorization of all individuals accessing DCJIS resources. The Agency Head and CJIS Representative shall annually certify the accuracy of his/her agency's authorized user list to the DCJIS CSO.

11.0 Ownership of CJI Contained Within DCJIS Databases and Systems

The Source Agency will maintain ownership of, and responsibility for, the CJI it enters or modifies within any database or system operated, maintained, or managed by the DCJIS.

The Source Agency will exercise due diligence to ensure that the CJI it enters is current, complete, and accurate. Each Source Agency is also responsible for ensuring that the CJI it contributes is in compliance with all federal, state, and local laws.

User agencies shall communicate any errors found in CJI contained in any database or system operated, maintained, or managed by the DCJIS to the Source agency for that CJI as well as to the DCJIS.

12.0 Dissemination of CJI

CJI contained within, or obtained through, any database, system, or network operated, maintained, or managed by the DCJIS shall only be disseminated to other authorized agencies and individuals. In addition, the CJI obtained within, or obtained through, any DCJIS resource shall only be used for authorized justice or public safety purposes.

13.0 Public Records

Records maintained within the databases and systems operated, maintained, or managed by the DCJIS are subject to the Massachusetts Public Records Law as defined in M.G.L. c. 4, s. 7(26).

All responses to public record requests for information contained in a DCJIS resource shall be provided by the Agency that contributed the relevant information.

The DCJIS CSO may respond to a public records request for statistical data drawn from a DCJIS resource.

14.0 Data Submission and Retention Policy

Source Agencies shall contribute data to each DCJIS database or system pursuant to the schedule established in the Companion System Agreement for that database or system, if applicable. Companion System Agreements are attached to this Agreement as Addenda.

Data maintained in DCJIS databases and systems shall be retained pursuant to the schedule established in the Companion System Agreement for that respective system, if applicable.

15.0 Data Submission Standards

For each system that requires the contribution of data by Source Agencies, those Agencies shall submit at least the minimum set of data as established in the Companion System Agreement for the respective subject application.

16.0 Designation of an Agency Representatives

CJ/5 Representative:

Each agency accessing or using CJI obtained from or through the systems and networks operated, maintained, or managed by the DCJIS shall appoint a CJIS Representative. The CJIS Representative serves as the primary agency point of contact for the DCJIS.

Responsibilities include ensuring that all DCJIS system usage and security policies and procedures are being followed by the agency, training all agency personnel who access any system or network operated, maintained, or managed by the DCJIS or who use the CJI obtained from or through those systems and networks, and attending all DCJIS-sponsored meetings, seminars, and conferences.

Backup 015 Representative:

Each agency that accesses or uses CJI obtained from or through the systems or networks operated, maintained, or managed by the DCJIS shall also appoint a Backup CJIS Representative. The Backup CJIS Representative shall be the DCJIS' secondary point of contact for the agency. In addition, the Backup CJIS Representative shall assume all of the duties and responsibilities of the CJIS Representative should the CJIS Representative be unable to perform those duties and responsibilities for any reason.

015 Technical Representative:

Each agency accessing or using CJI obtained from or through the systems and networks operated, maintained, or managed by the DCJIS shall appoint a CJIS Technical Representative. The CJIS Technical Representative serves as the primary agency point of contact for the DCJIS on all technology-related matters. The Technical Representative's

main responsibility is to ensure that the agency meets the requirements of the FBI CJIS Security Policy. The CJIS Technical Representative may also serve as either the CJIS Representative or the Backup CJIS Representative.

17.0 Technical Support

The Executive Office of Public Safety and Security (EOPSS) Office of Technology and Information Services (OTIS) shall provide technical support services for all applications, databases, systems, and networks, operated, maintained, or managed by the DCJIS.

18.0 Internal Agency Policies

Each agency obtaining CJI either directly from, or through, an application, database, system, or network operated, maintained, or managed by the DCJI shall draft and adopt internal policies to inform and ensure that agency authorized users have read and agree to comply with the provisions of this Agreement and its Addenda.

19.0 Termination of Access

A agency may request termination of its access to one or more DCJIS resources by providing a written request to the DCJIS CSO.

The DCJIS CSO may also terminate access to a DCJIS resource pursuant to the terms of a Companion System Agreement.

20.0 Amendments

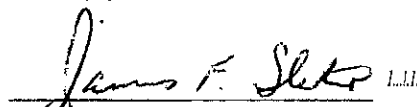
Any change in the provisions of this Agreement or in the provisions of a Companion System Agreement shall be incorporated by a written amendment approved by the DCJIS CSO.

21.0 Global Justice and Public Safety User Agreement Signoff

By signing this Agreement, the Agency Head acknowledges he/she has read and understood its provisions and that he/she will comply with its terms and conditions.

Agency Head

Date



DCJIS Commissioner
1/5/2011

/ /

Date



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 through, 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.