OFFICIAL ORDER
MICHIGAN STATE POLICE

SUBJECT: Policy Governing the Use of License Plate Reader Systems

TO: Department Members

This Order establishes department policy and member responsibilities for the following:

28.1 POLICY GOVERNING THE USE OF LICENSE PLATE READER SYSTEMS

This policy governs the use of automated License Plate Reader (LPR) technology by members.

28.1.1. Definitions

A. Access: For the purposes of this policy, access is the ability to receive LPR Data through Target Alert System (TAS).

B. Administrators: Administrators are those defined as having full access rights to the LPR system. Administrators may be responsible for audits, credential/access rights monitoring, and defining roles as permitted by the LPR policy and Michigan State Police (MSP)

Command approvals. Administrators will also be responsible for maintaining the whole LPR system throughout the state of Michigan.

C. Active LPR Data: Active LPR Data is information which is provided to a law enforcement official in real-time. Active LPR Data includes:

(1) Alerts or notifications that a license plate number contained on an Alert List has been detected in the vicinity of an LPR Unit.

(2) Mobile LPR Data collected and recorded during a law enforcement official's shift and accessible from within the patrol car that has not previously been downloaded into a database of Historical LPR Data.

(3) Shared data is collected from an outside agency that is law enforcement sensitive. Shared information is not owned by the department but used for law enforcement investigations. A Memorandum of Understanding (MOU) must be submitted to the department for approval before any information can be shared or collected.

D. Alert List Data: Alert List Data consists of license plate numbers selected by the department for inclusion on a particular list to facilitate the identification of vehicles displaying those license plate numbers.

E. Credentials: As used herein, the term credentials shall mean login information that corresponds with a sole individual's access to an LPR system. This information is personal in nature and is held to the same requirements as found in Official Order No. 21, the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy and the State of Michigan (SOM) Technical Standard, 1340.00.130.02 Acceptable Use of Information Technology.

F. Crime: As used herein, the term "crime" shall mean an act or the commission of an act that is forbidden or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law. The term "crime" includes acts of terrorism.

G. Dissemination Log: Refers to a gathering of information pertaining to the LPR data that has been released to the public per orders of the public safety exception for historical data.

H. Historical LPR Data: Historical LPR Data consists of the dates, times, and locations of individually identifiable motor vehicles that is stored for future use and includes any LPR Data not considered Active LPR Data.

I. Jurisdiction: The geographical territory within which a law enforcement agency may exercise its power to enforce the law. This territory is defined as being within the state of Michigan.

J. Law Enforcement Information Network (LEIN)/National Crime Information Center (NCIC) Alert List: LEIN/NCIC Alert List mean the list of license plates and certain other data extracted from the LEIN Alert Files and combined with the NCIC LPR Alert List.

K. LPR Alert Entry: An LPR Alert Entry is entering a known license plate with a criminal predicate into the LPR System.

L. LPR Data: LPR Data consists of all LPR images and/or alerts that are active or historical in nature and stored within the LPR System.

M. LPR Images: LPR Images consist of the optical appearance of the license plate and the surrounding area of the front and/or rear of a motor vehicle. LPR Images include information that is not rendered into an electronically readable format.

N. LPR System: LPR System consists of the LPR Units, communications network components, data server hardware, and software including any Optical Character Recognition (OCR) software and algorithms, all operating in an organized and coordinated manner.

O. LPR Units: LPR Units consist of the imaging hardware which captures the image of the license plates, regardless of the types of cameras used or the deployment of the unit.

P. Managers: Managers are those defined as having credentials to the LPR system for the purpose of searching license plates for investigations as defined below. Managers may also be granted access rights to the system for the purpose of receiving TAS alerts from Alert Lists.

Q. Memorandum of Understanding (MOU): Refers to any agreement between the department and other law enforcement agencies.

R. Query Response: A Query Response consists of the data provided by the LPR System in response to a transaction initiated by an authorized user.

S. Real-time: As used herein, the term "real-time" means a system in which input data is processed so that it is available virtually immediately.

T. Statistical Summary Data: Statistical Summary Data consists of a summary set of observations concerning Historical LPR Data, which includes, but is not limited to:

(1) Measures from location(s), (i.e., average location, average number of license plate scans, average number of Alert-List hits).

(2) Raw counts of LPR Image captures. Statistical Summary Data shall not contain any license plate numbers.

U. Supervisors: Supervisors are those defined as having credentials for the LPR system to both search and enter license plates into the system as directed by the LPR policy. Supervisors may also be granted access rights to the system for the purpose of receiving TAS alerts from Alert Lists.

V. Users: Users are those defined as having access to the LPR system for the purposes of TAS alerts. These users will not have credentials for the system.

28.1.2. Purpose for Collecting LPR Data

A. LPR Data may be collected:

(1) To support crime analysis techniques.

(2) To alert law enforcement officials of the proximity of a vehicle displaying a license plate number that is included on an Alert List.

(3) To locate vehicles displaying particular license plate numbers and letters that has a known relationship to an individual who is reasonably suspected of having committed a crime.

(4) To help law enforcement officials detect unreported and previously undetected crimes.

(5) To help law enforcement assist in locating missing or endangered persons and/or juveniles.

28.1.3. Collection of LPR Data

A. LPR Units may be deployed within the department's jurisdiction in any one or all the following manners:

(1) In a Fixed Deployment, by being permanently mounted in a fixed location.

(2) In a Portable Deployment, by being semi-permanently placed, whether overtly or covertly; or

(3) In a Mobile Deployment, by being mounted to a mobile vehicle, whether overtly or covertly.

(4) All fixed and mobile LPR equipment shall require Field Operations Bureau (FOB) approval before acquiring and deploying such equipment.

(5) District-level authorization is required for deployment of Portable LPR Units.

B. Elements of LPR Data

(1) Each piece of LPR Data collected by the MSP must include:

a. The LPR image.

b. The license plate number derived by the system's OCR software.

c. The Global Positioning System (GPS) coordinates or other location information of the observation.

d. The date and time of the observation; and

e. The deployment configuration of the LPR Unit that captured the LPR image.

(2) Each piece of LPR Data collected by the department may include other information that aids in the identification of vehicles including, but not limited to, the non-electronically readable information contained in the LPR image (i.e., color, make, model, truck cap, etc.).

(3) LPR Data is not considered personal identifying information.

C. The department shall maintain control of retention and dissemination of historical LPR data per departmental retention and disposal schedules.

28.1.4. Credentials and Dissemination of LPR Data

A. The department credentials to the LPR system shall follow the below listed guidelines.

(1) Members shall not have access granted through any other department's LPR system at any time.

(2) LPR access for members is reserved only for the department's LPR maintained system and credentials or access may be granted in accordance with guidelines defined below.

(3) Once a member has transferred or ended employment, those granted access or credential rights shall be terminated.

(4) Users shall not share any credential or access log in information as this information is personal in nature and is held to the same requirements as found in Official Order 21, the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy and the State of Michigan (SOM) Technical Standard, 1340.00.130.02 Acceptable Use of Information Technology.

B. Unless a request for an elevated designation has been submitted through the chain of command for approval by a bureau commander, or a bureau commander's designee, the access designations will be assigned to the corresponding departmental positions as follows:

(1) Users: Authorized troopers and motor carrier officers

(2) Managers: Hometown Security Team personnel, authorized sergeants, Task Force members at a Lieutenant 14 level, and Michigan Intelligence Operation Center (MIOC) analysts

(3) Supervisors: Regional Communication Center emergency dispatchers and lieutenants in the MIOC Operations Section

(4) Administrators: Administrators will be selected by a bureau commander or their designee.

C. Anyone not employed by the department and not identified above, shall not be granted credentials to the LPR system. LPR Data can be shared upon written request to any personnel listed above with confirmation of an ongoing criminal investigation. Federal agencies can access LPR data through their federal identified database.

D. LPR Alert Entries may only be made by those having LPR credentials and having been approved by Administrators/Bureau to enter a license plate in accordance with departmental policy. All LPR Alert Entries shall be entered into the MSP LPR System and not through any other LPR System. LPR Alert Entries shall only be made for the purpose of making contact and/or surveilling a vehicle immediately upon receiving an alert. Queries of other LPR Systems are permitted.

E. Members with LPR system credentials and authorized troopers and motor carrier officers may access LPR Data for the purposes of:

(1) To detect stolen vehicles displaying license plates located or operated in the vicinity of an LPR unit.

(2) To detect vehicles displaying license plates reported as stolen.

(3) To detect vehicles displaying license plates reasonably related to individuals identified as wanted.

(4) To detect vehicles displaying license plates reported as associated with violent felonies of child abductions.

(5) To detect vehicles displaying license plates contained on an Alert List.

(6) For any official law enforcement investigative purpose.

F. Members with LPR System credentials may access Historical LPR Data:

(1) To conduct crime analysis.

(2) To identify and track the movement of vehicles displaying license plates reasonably related to a crime that has already been committed.

(3) To identify and track the movement of vehicles displaying license plate numbers contained in an Alert List.

(4) To identify and track the movement of vehicles displaying license plates reasonably related to individuals when there is articulable suspicion linking the individual to having committed a crime.

(5) To generate investigative leads for the investigation of a felony.

(6) To detect instances of criminal conduct not previously observed or reported to the MSP; and

(7) To otherwise investigate crimes and criminal conduct.

G. Disseminating Historical LPR Data to Law Enforcement Agencies.

(1) Upon receiving a written request, and documenting that request, for Historical LPR Data pertaining to certain license plate numbers, Historical LPR Data may be disseminated to law enforcement officials from other jurisdictions.

(2) The department shall not disseminate Historical LPR Data in a bulk manner absent an approved MOU with a law enforcement agency.

H. Limited Dissemination of Historical LPR Data to Other Government Entities.

(1) Statistical summary LPR Data may be disseminated to government entities that are not also law enforcement agencies.

(2) LPR Data related to a specific license plate number shall not be disseminated with government entities that are not also law enforcement agencies.

I. Non-Dissemination of Historical LPR Data to the Public.

(1) Expect as provided below, LPR Data shall only be used for law enforcement purposes. LPR Data shall not be released to the general public, unless required by statute or court order. The Records Resource Section shall raise any and all applicable exemptions contained in the Freedom of Information Act, MCL 15.231 et. seq., to withhold or otherwise limit the disclosure of Historical LPR Data.

(2) Historical LPR Data shall not be disseminated to members of the general public or news media. This prohibition is subject only to the exceptions set forth in paragraphs (3) through (4) of this Section.

(3) Where the head law enforcement official or the elected prosecutor of a jurisdiction reasonably determines that an individual or vehicle poses a threat of substantial harm

to the public, LPR Data may be released to the public, including, but not limited to, private security personnel.

a. A determination that the public safety exception at Section 28.1.4.I (3) applies must be documented in writing and retained in the same manner as a dissemination log.

b. The release of LPR Data must be limited to information that could reasonably protect the public from the harm justifying the dissemination of the data.

(4) LPR Images may be used in a photo line-up to further a specific investigation for which the LPR Image was requested.

J. Dissemination of Active and Historical LPR Data, other than as set forth in Sections 28.1.4. F through and including 28.1.4. H, is prohibited.

K. Statistical Summary Data of the department's Historical LPR Data may be disseminated notwithstanding the limitations imposed on Active and Historical LPR Data.

L. Administrative rights may be granted through a formal request to the MSP FOB. Administrative rights shall be limited to persons identified within the Michigan Intelligence Operation Center, FOB, and/or the Information Technology Division, and should be limited to areas of work that are identified in the request.

28.1.5. Retention of LPR Data

A. LPR Data connected to a criminal investigation, including but not limited to Query Responses, shall be retained as part of the investigation record and shall be subject to department retention and disposal schedules.

B. LPR Data used to convict an individual, including but not limited to Query Responses, shall be retained as part of the MSP's case file as an external document and shall be subject to department retention and disposal schedules for that specific case and conviction.

C. LPR Data that is not connected to an investigation or conviction shall be subject to departmental retention and disposal schedules.

D. Statistical Summary Data shall be retained pursuant to the departmental retention and disposal schedule.

E. Automated audit logs of LPR system activities, system settings, Alert List changes, data queries, and query responses shall be subject to departmental retention and disposal schedules.

28.1.6. Quality of LPR Data

A. The department shall monitor the quality of the LPR Data it maintains, uses, analyzes, and disseminates regardless of its source.

(1) MSP officials, utilizing Historical LPR Data, who identify an inconsistency between the LPR Image, and the license plate number derived from the LPR Image by the OCR software shall take steps to correct the LPR Data.

(2) MSP officials utilizing Active LPR Data shall visually confirm, either from the LPR Image or the license plate itself, that the license plate which caused the LPR System to generate an alert or notification matches the information contained in an Alert List

prior to taking any enforcement action other than following the vehicle. See LPR Operational Guidelines for full details.

B. The department shall ensure the most recent or most trusted software is installed and used by the LPR System.

C. The department shall conduct routine data quality audits to measure the accuracy of the OCR output derived from LPR Images.

D. Individuals have no right to access or challenge LPR Data unless otherwise authorized by law.

28.1.7. Alert List Program

A. The department may compile Alert Lists that further the department's mission and public safety goals. Each Alert List shall be compiled and implemented as follows:

A documentable record supporting each license plate's inclusion on the department's Alert List, consistent with the reasons for the use of Active and Historical LPR Data contained in Section 28.1.4. B of this policy.

B. The Administrator of the department LPR program shall determine which Alert Lists are uploaded into the MSP's LPR System.

C. Prior to detaining a vehicle or individual based upon an alert or notification that the vehicle's license plate number is on an Alert List, the law enforcement official shall verify that the vehicle's license plate number, obtained from a visual inspection of the plate or the LPR Image, matches the information contained on the Alert List.

D. Prior to detaining a vehicle or individual based upon an alert or notification that a vehicle's license plate number is on the LEIN/NCIC Alert List, the law enforcement official shall run the license plate number in LEIN and NCIC to ensure the vehicle/license plate is an active record.

E. Retention of Alert List Data.

(1) All Alert List Data is subject to the department's retention and disposal schedule.

(2) Alert List Data connected to an investigation shall be retained as part of the investigation record and shall be subject to the departmental retention and disposal schedule.

(3) Alert List Data used to convict an individual shall be retained as an external document and in accordance with the department's retention and disposal schedule.

F. MSP officials utilizing Alert Lists who identify an inconsistency between the license plate number contained on an Alert List and the records supporting that license plate number's inclusion on the Alert List shall take steps to correct the Alert List.

G. Individuals have no right to access or challenge Alert List Data unless otherwise authorized by law.

28.1.8. Accountability for LPR Data

A. The department shall monitor the use of the LPR System, including but not limited to Alert List changes, individual searches, LPR data access, and the dissemination of Historical LPR Data.

B. Policy Awareness and Training

(1) Training shall be provided to individuals prior to accessing, maintaining, analyzing, or otherwise utilizing the department's LPR Data on the following topics:

a. The requirements contained in this Order and the importance of complying with its terms.

b. The types of errors LPR software can make when extracting electronically readable information from an LPR Image.

c. LPR Data relates only to a vehicle's license plate information whereabouts and not necessarily the whereabouts of its registered owner; members shall follow the operational guidelines as set in this policy.

d. A license plate number is not a proxy for an individual's name or other personally identifying information; and

e. Any additional subjects the department considers significant to ensure LPR Data is appropriately accessed, analyzed, and disseminated.

(2) Use of the department's LPR System shall be limited to members who have completed training in accordance with this section and provide documentation of successfully completing that training.

(3) The department shall maintain appropriate records confirming personnel that access or utilize LPR Data have completed training in accordance with this Section.

C. The department shall monitor relevant legislative and regulatory activity impacting the administration of LPR Systems or the collection, analysis, and dissemination of LPR Data and shall update this Policy accordingly.

28.1.9. Security of LPR System and Data

A. The site security, system integrity, personnel security, and system security of the LPR system and data shall be maintained in accordance with Official Order No. 21, the FBI CJIS Security Policy, the FBI CJIS Security Policy Michigan Addendum, and SOM Policy 1340.00 Information Technology Information Security.

28.2 REVISION RESPONSIBILITY

Responsibility for continuous review and revision of this Order lies with the Field Operations Bureau and Field Support Bureau, in cooperation with Executive Operations.

DIRECTOR