2.455 AUTOMATED LICENSE PLATE RECOGNITION (ALPR)

2.455.10 PURPOSE AND SCOPE

Automated License Plate Recognition (ALPR) uses infrared technology to scan, detect and identify license plate numbers.

The purpose of this policy is to provide guidance for the capture, storage, and use of the digital data obtained through the use of the ALPR technology.

2.455.15 OPERATIONS

Use of the ALPR is restricted to the purposes detailed below.

Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose. ALPR shall be used only for official and legitimate law enforcement business.

ALPR may be used in conjunction with any routine patrol function or criminal investigation. Reasonable suspicion or probable cause is not required before using ALPR.

Users are encouraged to enter license plate numbers manually into "Hot List" when a vehicle is suspect or wanted, such as in major investigations or Amber Alert (or other similarly designated alerts). ALPR can be used to canvass license plates around any crime scene in real time to attempt to identify suspect or witness vehicles, or both. The ALPR database of stored scans may be searched for specific dates, times, and locations of open investigations for vehicles of potential interest.

Generally, members should not take enforcement action based solely on an ALPR alert to a mobile data computer. Members are expected to verify, whenever practicable and safe, any ALPR information through the appropriate source before taking action.

2.455.20 TRAINING

Members shall not operate ALPR equipment, nor access data, without first completing department-approved training and any other instruction mandated by the California Department of Justice (DOJ), to include that pertaining to CLETS access.

Training coordinators designated by the department should ensure members intended to use ALPR equipment and access the databases receive appropriate and mandatory training (California Civil Code 1798.90.51, and California Civil Code 1798.90.53).

2.455.25 USER RESPONSIBILITY

At the beginning of each tour of duty, users shall inspect ALPR terminals and operability. They shall document and immediately report to a supervisor any problem or damage.

During their tours of duty, users, while in their vehicles, will monitor all reads and any possible matches. Users should, when practicable and safe, verify for accuracy any possible matches.

Members shall not make, nor allow to be made, modifications to the ALPR system, software, or system configuration. Nor, shall they allow the ALPR system to be connected to any other devices.

Unauthorized members shall not access ALPR data.

Members authorized to access ALPR data shall do so only when it relates to a specific criminal investigation, or an administrative or civil action related to the department. Data may be shared only with law enforcement or prosecutorial agencies.

2.455.30 DATA COLLECTION AND RETENTION

ALPR data downloaded to the server shall be stored for a minimum of one year (California Government Code Section 34090.6). The department shall maintain the data for two years. Data will be purged after two years unless it is, or it is reasonable to believe that it will become, evidence in a criminal or civil action; or, is subject to a lawful order to produce records. The department shall, under those circumstances, preserve applicable data on portable media, which then shall be entered into evidence.

2.455.35 ACCOUNTABILITY AND SAFEGUARDS

Data and images gathered by ALPR are for the department's official use. Because this data has the potential for misuse, it is not open to public view.

Transmission and storage of data shall meet CLETS' requirements for network and computer security.

Saved data shall be safeguarded and protected by both procedural and technological means. ALPR data downloaded to mobile workstations or servers shall be accessible only through a log-in password protected system.

Authorized members shall access the system only to participate in department-approved training; or, to retrieve stored data related to a specific criminal investigation, or to an administrative or civil action related to the department. Articulable suspicion must exist that stored data is related to one of these investigative purposes.

Access or use of the ALPR data for other reasons may be cause for formal discipline or criminal prosecution.

2.455.40 RELEASE OF DATA

ALPR data gathered and retained by the department may be used and shared with prosecutors and other law enforcement agencies only as permitted by law. Data gathered by the ALPR shall not be released to a non-law enforcement entity.

2.455.45 DISCLOSURE OF BREACH OF SECURITY

California law (Civil Code section 1798.29) requires any agency that owns or licenses computerized data that includes personal information to disclose any breach of security, following its discovery, to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The law requires such disclosure to be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of the law enforcement agency. The disclosure shall be written in plain language.

It shall be the responsibility of the Commander of the Information Services Division to develop appropriate procedures to ensure compliance with these requirements, and to ensure such written notice is timely delivered.

2.455.50 ADMINISTRATION

The Commander of the Information Services Division shall be responsible for developing and maintaining written guidelines and procedures to ensure compliance with the requirements of California Civil Code section 1798.90.5 and all of its subsections.

These guidelines and procedures shall include, but are not limited to:

- A description of the job title or other designation of the members and independent contractor authorized to use or access the ALPR system, or to collect ALPR information;
- Training requirements for authorized users;
- A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws;

- Procedures for system operations to maintain records of access in compliance with California Civil Code section 1798.90.52;
- The title and name of the current designee overseeing the ALPR operation;
- Coordination with the custodian of records for the retention and destruction of ALPR data;
- Random user audits and reports from system administrators.

The Commander of the Information Services Division also shall all ALPR policies and procedures required by law are conspicuously posted on the department's website.