CALIFORNIA HIGHWAY PATROL

GENERAL ORDER 60.1

REVISED JULY 2020

USE OF AUTOMATED VEHICLE LOCATOR SYSTEM DATA

1. PURPOSE. The purpose of this General Order is to establish standardized policies and procedures regarding the use of Automated Vehicle Locator System (AVLS) data. This policy applies to no other means of location data compilation.

2. GENERAL. The AVLS is a means for automatically determining the geographic location of a vehicle and transmitting the information to a requester. The use of AVLS data has proven to be a valuable tool for law enforcement agencies in their service to the public and for the safety of their officers. The AVLS uses Global Positioning Satellite data to locate each patrol vehicle using latitude and longitude coordinates, as well as noting the vehicle's speed. This data is refreshed every 30 seconds, providing almost real-time information. Therefore, the AVLS shall not be used solely to determine a patrol vehicle's speed. However, in the case of an officer emergency, such as an officer who is missing or does not answer in response to a roll call, assistance can be quickly dispatched to the last known location using AVLS data for the vehicle involved. The data can also be used to establish perimeters at major incidents visible in the Computer Aided Dispatch (CAD). Additionally, the data can be very helpful when used in after-action reports of incidents, such as pursuits. It is the intent of the California Highway Patrol (CHP) to provide this data to enhance officer safety and service to the public.

3. POLICY. The AVLS data is available to dispatch, uniformed, and supervisory personnel. The AVLS data may be viewed if there is an operational need to do so. However, the data should not be viewed if there is not a demonstrated call for the data. All personnel who have access to the AVLS, and those who supervise or manage such personnel, shall review this policy on an annual basis. Policy review shall be documented on each employee's training record at the time of their annual performance review.

   a. Dispatch Personnel. The AVLS data shall not be routinely viewed as part of the dispatch screens. This does not preclude the use and viewing of unit locations on the dispatch map screen.

(1) While in a Unit Activity Log within VisiCAD during normal dispatch activities, the “Show AVLS Data” box shall remain unchecked so as to make the data unavailable for viewing.

(2) The “Other Information” tab within each Unit Detail screen describing the patrol vehicle and AVLS data will not be accessed unless there is a clearly identified operational need or with supervisory approval.

b. Uniformed Personnel. The AVLS data shall not be routinely accessed on the Mobile Digital Computer or on the VisiNET Web browser during a patrol shift.

(1) Uniformed personnel may access AVLS data for their own patrol vehicle if they have the need to do so.

(2) Uniformed personnel may access AVLS data for a patrol vehicle other than their own if there is an emergency where the data is needed to locate another officer.

(3) Uniformed personnel may review AVLS data as part of an after-action report of an incident, such as a pursuit, if a demonstrated need can be articulated outlining the benefits of having the data.

c. Supervisors and Managers. The AVLS data may be reviewed as part of an investigation or if needed to complete incident reports. The data shall not be routinely reviewed to generate monthly and/or annual employee performance evaluations, nor shall the data be randomly viewed for the sole purpose of locating policy and/or criminal violations. It is the responsibility of the supervisors and managers of uniformed and dispatch personnel to ensure that they have a demonstrated reason to recall and view the data.

4. CRIMINAL, CIVIL, AND ADMINISTRATIVE PROCEEDINGS. There may be occasions where AVLS data will be requested as part of a criminal, civil, or administrative proceeding. The policies and procedures relating to disclosure of public records and rights to privacy, as well as subpoena duces tecum, as contained in Highway Patrol Manual 11.1, Administrative Procedures Manual, shall be followed.

a. Criminal Proceedings. Copying, viewing, and release of AVLS data maintained for evidence in criminal proceedings shall be coordinated through the district attorney’s office.

(1) The existence of AVLS data collected and retained as evidence, by dispatch or a field command, for possible civil litigation must be disclosed to the prosecutor in a criminal proceeding. However, release of that data is protected by attorney-client privilege. Copying, viewing, and releasing of the

data shall be coordinated through the Office of Legal Affairs, Case Management Unit.

b. Civil Proceedings. Copying, viewing, and releasing data shall be coordinated through the office of Legal Affairs, Case Management Unit.

c. Administrative Proceedings. The AVLS data may be used by the Department for the purposes of proving and disproving allegations of misconduct. Only that data relevant to the investigative scope shall be viewed and retained by investigators. This information can be located through the VisiNet Web browser. Information relevant to the data viewed and seized as evidence by investigators shall be documented as part of the chronological summary of a criminal or internal investigation. Upon request, employees subject to discipline, as defined by Government Code §19572, shall be provided a copy of the data utilized to support administrative sanctions upon being served with a notice of adverse action.

5. USE OF AUTOMATED VEHICLE LOCATOR SYSTEM DATA FOR TRAINING PURPOSES. When an incident is perceived to be of value as a training aid and the AVLS data can add value to the training, the uniformed or dispatch employee may report that belief to their supervisor who will review the data to determine the value of the incident for training. If the supervisor determines the incident would be an appropriate training aid, and the incident is not part of an ongoing criminal/civil proceeding, AVLS data may be used at the discretion of the Area commander. Additionally, public safety dispatch training personnel may access real-time AVLS data when conducting public safety dispatch training.

6. RETENTION OF DATA. The CHP CAD is a sophisticated product designed to provide real-time access to data, while still meeting the subsecond response time requirements. To accomplish this, the CAD data is spread across three databases:

a. First Tier. The production CAD database keeps all data for 90 days for real-time access.

b. Second Tier. The Data Warehouse keeps all data for 90 days for reporting access and some real-time data.

c. Third Tier. The CHP Central Reporting System (CRS) keeps all data for one year for large-scale reporting.

(1) The third tier of the CAD database exists because the CHP has two Divisions in each of the four CAD hubs. To enable reporting across all the CHP data, the CRS must be queried as it contains CAD data from all Divisions.

7. PURGING OF DATA. It is necessary to periodically purge data from each of the databases. The purge parameters are set to avoid unintended consequences and unnecessary changes to the CAD systems.

a. The purge of the first tier database (Production CAD) is done on a weekly basis and purges all CAD data in that database older than 90 days.

b. The purge of the second tier database (Data Warehouse) is run weekly and purges all AVLS information from that database older than 90 days.

NOTE: The Production CAD and Data Warehouse purging removes the AVLS data from all CAD users within one week after the data is 90 days old. Therefore, there will be times when data on each database is up to 96 days old.

c. The CRS database is purged weekly and purges all AVLS data more than one year old. Purging after one year matches the current CHP retention period for electronic CAD data on the State of California STD. 73, Records Retention Schedule, submitted to Department of General Services.

d. The purging of AVLS data is not to be confused with the California Law Enforcement Telecommunications System (CLETS) requirement to retain all Message Switch log data for a minimum of three years (CLETS Policies, Practices and Procedures dated June 2018, Section 1.7.1). The CLETS data is retained in the Message Switch and is not part of the CAD data purge.

OFFICE OF THE COMMISSIONER

OPI: 047