CHAPTER 6

CALIFORNIA LAW ENFORCEMENT TELELCOMMUNICATIONS SYSTEM

REVISED NOVEMBER 2021

TABLE OF CONTENTS

CHAPTER 6

CALIFORNIA LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM

1. GENERAL.

a. Purpose. The California Law Enforcement Telecommunications System (CLETS) is a message switching system under the control of the California Department of Justice (DOJ). The CLETS provides access to a variety of information services at the state, interstate, and federal levels, and is accessible by authorized departmental personnel.

b. Accessibility.

(1) The CLETS can be accessed via various devices and applications on the CHP network.

(a) Web Workstation. This application is on CHP's local area network (LAN), and is available in Division, Area, communication and dispatch centers, Commercial Vehicle Enforcement Facilities (CVEF), scales, and headquarters locations. Requests to access this application can be made through the CHP Information Technology (IT) Support.

(b) Computer Aided Dispatch. This application is available in communications and dispatch centers. Access is provided, upon hire, for dispatch personnel. Other requests to access this application can be made through the CHP IT Support.

(c) Mobile Digital Computers. These are mobile devices used in vehicles, on laptops, and on tablets using the mobile application. Access is provided, upon hire, for new uniformed personnel. Other requests to access this application can be made through CHP IT Support.

c. Databases.

(1) Department of Justice CLETS databases:

(a) Stolen Vehicle System (SVS).

(b) Automated Boat System (ABS).

(c) Wanted Persons System (WPS).

(d) Automated Property System (APS).

(e) Automated Firearms System (AFS).

(f) Missing and Unidentified Persons System (MUPS).

(g) Supervised Release File.

(h) Armed and Prohibited System.

(i) Criminal History System (CHS).

(j) Mental Health Firearms Prohibition System (MHFPS).

(k) California Restraining and Protective Order System (CARPOS).

(l) California Sex and Arson Registry.

(2) The Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC).

(3) The National Law Enforcement Telecommunications System (NLETS).

d. California Law Enforcement Web Site. The DOJ's California Law Enforcement Web site is an Internet site for CLETS users. The site can be accessed at http://clew.doj.ca.gov/. All employees shall use their departmental e-mail address and the Originating Agency Identifier (ORI) of their location when requesting a sign-on and password.

e. The CHP has information on CLETS, including publications and forms, which can be found on the CHP Intranet site, under Resources, Technology, CLETS.

2. ROLES AND RESPONSIBILITIES.

a. Management Control. Management control over access and use of CLETS is governed by Government Code Sections 15150-15167 and the DOJ CLETS Policies, Practices, and Procedures (PPP) (and Statutes). Government Code Section 15153 states CLETS shall be used exclusively for official business. Any use of CLETS for functions other than conducting CHP business is a violation of this section.

b. Operational Control. The Information Management Division (IMD), Communications Centers Support Section (CCSS), has been delegated the responsibility for operational control and system management of CLETS. The CCSS is also the Office of Primary Interest for matters relating to CLETS security, policy, and training.

c. System Administrator. One position in CCSS has been designated as the CHP CLETS Administrator. The DOJ refers to this position as the Agency CLETS Coordinator (ACC). This individual serves as the Department's coordinator with DOJ relating to CLETS use and CLETS-supported administrative network and databases. Some of the primary responsibilities of the ACC include:

(1) Maintaining copies of the Department's CLETS applications and subscriber agreements signed by the CHP Commissioner, along with copies of all contractual CLETS agreements.

(2) Identifying and advising management of compliance issues with CLETS, Criminal Justice Information System (CJIS), NCIC, and NLETS policies and regulations.

(3) Maintaining the CLETS master departmental employee training, testing, and recertification records.

(4) Ensuring compliance with mandated state and federal auditing requirements, and referring audit information to the proper departmental resource.

(5) Maintaining information on CLETS terminal mnemonics and locations along with a current system diagram.

(6) Coordinating with DOJ on terminal access level changes, the request of additional CLETS mnemonics, and submission of applications for upgrading service.

(7) Ensuring the accuracy of CLETS user security files.

(8) Coordinating CLETS audits and/or inspections with DOJ staff.

(9) Notifying DOJ of address and telephone number changes.

(10) Coordinating and/or responding to CLETS-related correspondence.

(11) Assisting terminal operators with the use of CLETS formats.

(12) Coordinating the yearly report on the number of CLETS misuse investigations.

d. Area Commanders.

(1) Adherence to Policy. Commanders are responsible for implementation of and adherence to the policy outlined in this manual and in the manuals of the

DOJ and FBI which relate to the use of CLETS and NCIC. Compliance issues may be provided to commanders by the DOJ, FBI, the CHP CLETS Administrator, or other departmental management. Policy is applicable regardless of the means used to access CLETS (i.e., through Web Workstation [WebWS], Computer Aided Dispatch [CAD], Mobile Digital Computers [MDC], tablet, or any future methods which may be implemented).

3. POLICY.

a. Criminal Offender Record Information.

(1) Criminal history information has various names and references associated with it.

(a) The CHS is a DOJ database containing criminal history information.

(b) Automated Criminal History System (ACHS) refers to the access of criminal history information via an automated method, such as CLETS.

(c) Criminal Offender Record Information (CORI) refers to criminal history information and is not specific as to how it was accessed (e.g., fingerprints or automated).

(d) Interstate Identification Information is criminal history information obtained from the FBI's NCIC.

(e) Criminal history information is more protected and has more restrictions than information from other DOJ databases. Additionally, using criminal history information obtained online has even more restrictions.

(2) The CLETS shall not be used to access criminal history information for the following purposes:

(a) Licensing, employment, or certification purposes, for CHP or any other department. This includes checks for preemployment background investigations for sworn peace officers and/or law enforcement personnel as specified in Penal Code Section 830, et al.

(b) For remotely accessing a record for review and/or challenge by a subject of a record.

(c) Background checks for:

1 Concealed weapon permits for retirees or other persons.

2 Award recipients.

3 Tow truck drivers or candidates.

4 School bus drivers or candidates.

(d) Criminal history information for the above purposes shall only be obtained from fingerprint submissions.

(3) Inquiries.

(a) When making an inquiry into CHS via CLETS, users shall complete either the RETURN TO OFFICER/DIVISION field in WebWS (11-Criminal History Inquiry-CLETS and NCIC mask) or the RETURN TO or RTE field in CAD (Criminal mask), and ensure the following information is included:

1 The requester's ID number.

2 The operator's ID number (if different than requester).

3 The case number or other data specifying the nature or purpose of the request. Do not include general comments such as court officer, court liaison, criminal investigation, task force, etc. This field shall contain sufficient information to locate documentation for the inquiry, if requested.

(b) When making an inquiry into CHS via a system not belonging to CHP (i.e., the Los Angeles County Sheriff's Department's Justice Data Interface Controller [JDIC]), all mandates above apply and shall be followed. Additionally, since JDIC terminals utilize the ORI of the specific CHP Area, inquiries made via JDIC can be used when an audit is requested for that location.

(c) Tracking Inquiries. In addition to the requirement to log all releases of criminal history information, commands are encouraged to require staff to track all inquiries made into CHS. Tracking should include any errors made when making an inquiry, as audits will often include these when requesting documentation for inquiries.

(4) Releasing Criminal History Information. Pursuant to the California Code of Regulations, Title 11, Division 1, Chapter 7, Article 1, Section 707c, every agency is required to keep a record of each release of CORI for a minimum of three years from the date of release. A CHP 263B, Criminal Offender Record

Information Release Log, shall be maintained by all offices. Information for all releases of criminal history information outside of CHP, including to district attorneys, city attorneys, and courts, shall be stored on the CHP 263B and kept for a minimum of three years.

(5) Ride-Alongs and Sit-Alongs. A preliminary criminal history record check may be performed on any person prior to their approval as a "ride-along" with a law enforcement officer or "sit-along" with a CLETS operator, provided the person is not an employee of the law enforcement agency. Additionally, if that person is a prospective employee of the law enforcement agency, results of the online inquiry cannot be used for purposes of determining employment.

(6) Staff of any law enforcement facility may process online criminal history inquires on any visitor to such facility.

(7) Penal Code Sections 11120-11127 allow the subject of the record to obtain a copy of their state criminal history in order to ensure its accuracy and to refute any erroneous information it may contain. However, CHP **shall not** provide this information if requested. **The subject must complete an application and submit it to DOJ to receive this information.**

b. Confidentiality of Automated Information.

(1) Use of CLETS and related systems are governed by policy and statutes. Misuse of information obtained from CLETS may adversely affect an individual's civil rights and violate the law.

(a) Penal Code Sections 502(c)(1) and 502(c)(2) state: "Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

1 Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

2 Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network."

(b) Penal Code Section 502(d)(1) states: "Any person who violates any provisions of paragraph (1), (2), (4), (5), (10), (11), or (12) of subdivision

(c) is guilty of a felony, punishable by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years and a fine not exceeding ten thousand dollars ($10,000), or a misdemeanor, punishable by imprisonment in a county jail not exceeding one year, by a fine not exceeding five thousand dollars ($5,000), or by both fine and imprisonment."

(2) All information obtained via CLETS shall be cross or confetti-cut shredded and destroyed in a manner that prevents viewing or access by unauthorized personnel.

(a) California Law Enforcement Telecommunications System materials shall not be allowed outside of CHP presence, or control, at any time prior to shredding.

1 If an outside vendor or government entity shred materials, in the presence of CHP personnel, no further action or approvals are needed.

2 If an outside vendor or government entity shred materials, not in the presence of CHP personnel, the CHP location shall ensure all required documentation is completed in accordance with paragraph 3.g. of this chapter.

c. Limitation of Use and Access Requirements.

(1) Terminal Access.

(a) Access to CLETS on CHP workstations or devices by personnel from law enforcement and criminal justice allied agencies may be authorized on a case-by-case basis and must be approved by the CHP CLETS Administrator.

(b) Commanders shall ensure a completed CHP 101, Appropriate Use of Automated Information & Systems Statement, for each person accessing CLETS is placed in the command file.

(c) Commanders shall ensure a background investigation equivalent to that required of departmental employees is conducted and review the results. (Refer to paragraph 3.g. of this chapter.)

(d) Commanders shall ensure each employee has completed the appropriate CLETS/NCIC training, using CLETS Training and Recordkeeping System (CTARS), and Information Security and Privacy Awareness training.

(e) Each individual shall be assigned a unique six-digit user ID number, with a unique password, which shall be entered into the network table.

(f) Active CLETS records shall not be used for testing or training. Only DOJ "Test Records" shall be used for these instances.

d. Release of Information. Departmental personnel may release CLETS-provided information (verbal or written) to a law enforcement or criminal justice agency on a right-to-know, need-to-know basis under the following conditions:

(1) The release of CLETS information is authorized to the agency, which must be approved by the CHP CLETS Administrator.

(2) Examples of approved common releases include:

(a) The law enforcement or criminal justice agency does not have a CLETS terminal and the release is needed in the performance of the agency's official law enforcement-related duties. If requests are to be made on a continuing basis, the agency should be directed to the Contracts Unit in order to enter into a contract with CHP for these services.

(b) The agency has an existing contract for dispatch services with CHP, and the contract identifies that CLETS information is authorized to be provided. A listing of these agencies is available on the Dispatcher Resource Page.

(c) The law enforcement agency is experiencing problems with accessing CLETS and is in need of immediate CLETS information. It is the responsibility of the employee releasing the information to ensure the validity of the requester.

(d) The agency requires a printout of CLETS information as part of their business process, in conjunction with working with CHP (e.g., district attorney, city attorney, courts).

(3) Examples of **nonauthorized** releases include:

(a) Indian casino officers or employees.

(b) Toll bridge employees.

(c) A non-law enforcement agency or entity.

(d) Individuals with peace officer powers, who are not requesting on behalf of their employing agency (e.g., requesting for personal or secondary employment purposes).

(e) Any CLETS record for retired peace officers for purposes of reissuing concealed weapons permits.

(f) Any individual, with or without peace officer powers, that works for an agency that would not be approved by the DOJ. Check with the CHP CLETS Administrator to verify the requester is authorized to receive the information.

(4) Additional Requirements and Restrictions.

(a) Do not release CLETS-provided information to railroad police agencies, unless they are an authorized Guest User. Railroad police agencies are not considered public law enforcement agencies and must complete additional requirements. Contact the CHP CLETS Administrator before releasing any CLETS information to these agencies.

(b) Do not release CLETS-provided information on a routine basis to any agency that has a CLETS terminal. If CLETS-provided information is released, log the date, time, agency, requesting person, and reason.

(c) All releases of information should be to agencies approved for such release, as documented by the CCSS and the CHP CLETS Administrator.

(d) Unless under extenuating circumstances, criminal history information should not be released to any allied agency, including authorized Guest Users. If extenuating circumstances exist, the release of information shall be approved by a manager or supervisor.

(e) The release of criminal history information is permitted if required for the processing of CHP cases (e.g., district attorney, city attorney).

1 If criminal history information is to be accessed for an allied agency under extenuating circumstances, the purpose for the request shall be clearly identified (e.g., case number, type of investigation) prior to running the information.

2 If criminal history information is released outside of CHP, either verbally or written (including to an allied agency, district attorney, city attorney, courts, etc.), the details of the release shall be logged on the CHP 263B.

3 Running online criminal history information for the purpose of licensing, employment, or certification is never allowed.

(5) Obtaining approval for releasing CLETS information is the responsibility of the location releasing the information.

(a) For communications and dispatch centers:

1 A listing of authorized Guest Users is available on the Dispatcher Resource Page.

2 Requests for an agency not included in the listing must be verified by the CHP CLETS Administrator prior to releasing any information.

(b) For Division, Area, and CVEF offices:

1 Approval to release CLETS information to individuals working in a Joint Task Force-type of relationship is not needed.

2 Approval shall be obtained for all other releases and coordinated with the CHP CLETS Administrator prior to the release of information.

(6) Release of California Law Enforcement Telecommunications System Information Form. The DOJ has provided the HDC 0006, Release of Information from the California Law Enforcement Telecommunications System (CLETS), form for use by any agency when releasing CLETS information.

(a) Although the DOJ does not require the use of this form in all instances when releasing CLETS information, CHP has determined this form will be utilized with all dispatch contract relationships where CHP is releasing CLETS information.

(b) This form is required when releasing CLETS information to a non-CLETS subscribing agency. Contact the CHP CLETS Administrator to determine if a form is needed for a particular agency.

(c) The signature for CHP on this form shall always be the Commissioner and shall always be coordinated by the CHP CLETS Administrator.

(d) A Division, Area, or section wishing to provide CLETS information to a non-CLETS subscribing agency must coordinate the completion of this form with the CHP CLETS Administrator.

1 The Division, Area, or section commander shall:

a Check with the CHP CLETS Administrator first to ensure the agency is authorized to receive CLETS information.

b Obtain the signature of the head of the law enforcement section of the agency requesting the information and submit to the CHP CLETS Administrator.

2 The CHP CLETS Administrator will coordinate obtaining the Commissioner's signature and process the form.

(e) The form shall be updated when:

1 Either of the owners of the signatures changes.

2 Immediately upon request from the CHP CLETS Administrator.

e. Reciprocity Agreement. The HDC 0007, California Law Enforcement Telecommunications System (CLETS) Reciprocity Agreement, form is provided by the DOJ and is required for specific instances when an agency enters a record into CLETS for another agency.

(1) For the few instances where CHP has contracted with an agency to enter records on their behalf using the other agency's ORI, **the HDC 0007 is required**.

(2) The completion of this form shall be coordinated and approved by the CHP CLETS Administrator.

(3) No records of any type, including storages, shall be entered for any agency without prior approval and coordination of the CHP CLETS Administrator.

f. Interface Policy. Use of a terminal to obtain CLETS data for storage or transfer to a removable media is subject to the same security rules and procedures as data obtained through viewing a terminal screen or printed page.

(1) The DOJ/CLETS rules and regulations mandate all CLETS terminals and are subject to security and confidentiality restrictions. These rules and regulations apply equally to information obtained from the system either on screen, printed page, or removeable portable device. All system users are to comply with these rules and regulations statewide. Violations may be cause for dismissal and/or criminal prosecution.

g. Personnel Security.

(1) All personnel with unescorted access to CHP facilities are deemed to have access to CLETS information.

(2) Youth aids, student assistants, annuitants, senior volunteers, interns, and explorers are considered CHP employees. Their background shall be checked in the same manner as other permanent CHP employees, to include a DOJ and FBI fingerprint-based check and appropriate CLETS and Information Security and Privacy Awareness training.

(3) Private Contract Personnel. The following requirements apply when a private company is contracted by a CHP location, and the company's staff have unescorted access to CHP facilities:

(a) An HDC 0004B, CLETS Private Contractor Management Control Agreement, shall be completed. The CHP location will obtain the company owner's signature and forward the document to the CHP CLETS Administrator for processing.

(b) A California DOJ and FBI fingerprint-based CORI search shall be completed on all contract personnel with unescorted access to CHP facilities.

1 Any person with a felony conviction cannot be allowed access.

2 If any person has a felony arrest, without conviction, this information should be routed through channels to the appropriate Assistant Commissioner, to determine whether this person shall have unescorted access to CHP facilities.

(c) An FBI CJIS Security Addendum shall be signed by all contract personnel with unescorted access to CHP facilities.

(d) A CHP 101 or DOJ Employee/Volunteer Statement form shall be signed by all contract personnel with unescorted access to CHP facilities.

(e) Information Security and Privacy Awareness training shall be completed by all contract personnel with unescorted access to CHP facilities.

(f) A record of contract staff shall be kept, to include completion of all above requirements, and shall be available upon request.

(4) Other Agency (Government) Personnel. The following requirements apply when personnel from another state (Government) agency have unescorted access to CHP facilities:

(a) An HDC 0004A, CLETS Management Control Agreement, shall be completed. The CHP location shall check with CHP CLETS Administrator to determine if this form is already on file, or if the location must obtain one from the agency.

(b) A California DOJ and FBI fingerprint-based CORI search shall be completed on all persons with unescorted access to CHP facilities.

1 Any person with a felony conviction cannot be allowed access.

2 If any person has a felony arrest, without conviction, this information should be routed through channels to the appropriate Assistant Commissioner, to determine whether this person shall have unescorted access to CHP facilities.

(c) A CHP 101 or DOJ Employee/Volunteer Statement form shall be signed by all persons with unescorted access to CHP facilities.

(d) Information Security and Privacy Awareness training shall be completed by all persons with unescorted access to CHP facilities.

(e) A record of contract staff shall be kept, to include completion of all above requirements, and must be available upon request.

(5) Additional DOJ criminal justice databases may be accessed for background investigation of law enforcement and criminal justice employees, with the exception of ACHS and MHFPS.

(6) Periodic driver license checks may be conducted on CHP employees where driving is a requirement of their job.

(8) Visitors to a facility that has CORI access are not required to undergo a background and fingerprint-based CORI search. However, they must be escorted at all times, and shall not have visual or auditory access to any CLETS information.

(9) All employees shall read and sign the CHP 101 (refer to Chapter 2, Network Security and Administration, of this manual).

(10) Personnel shall not be given CLETS operator access until the required background and fingerprint checks are completed and approved by CHP, the required CLETS training has been completed, and the required form has been submitted indicating the specific access requested. Following approval of the completed investigation, place a memorandum or other notation in the employee's personnel file indicating CLETS operator access authorization has been granted.

(11) If the background or fingerprint check reveals a felony conviction of any kind, access to any CLETS information shall not be granted (which would prohibit unescorted access). If an arrest history without conviction for a felony is revealed, route the information through channels to the appropriate Assistant Commissioner who will review the matter and decide if CLETS access is appropriate.

h. Equipment Security.

(1) Personnel shall place terminals accessing CLETS in a secure location to provide protection from vandalism or sabotage and to preclude access by anyone other than authorized personnel.

(2) Personnel shall place terminals so screens are not visible to the public (e.g., on a front counter, other public area, or visible through an outside window).

(3) Personnel shall blank out terminal screens when visitors or tour groups are being escorted in the vicinity of terminals.

(4) All devices with CLETS access shall be secured to prevent unauthorized access. This includes locking the device or logging out of the CLETS application when away from the device.

(5) Any CHP device, and other hardware used for CLETS access (e.g., MDCs, laptops, tablets, servers, hard drives), shall not be transported outside of CHP custody, whether between CHP locations or elsewhere.

4. PROCEDURES.

a. Operating Procedures.

(1) The CLETS rules and procedures are designed to provide the most efficient operating methods consistent with the needs of all users.

(2) All formats and procedures specified in this manual and the manuals for using CLETS and NCIC are to be followed.

(3) Personnel shall not inquire into their own record or have someone inquire for them.

(4) Information from CLETS may be faxed from one secure location to another secure location. Both the agency faxing the information and the agency receiving the information are responsible for its security.

(5) Information from CLETS shall not be sent by e-mail, unless CLETS information has been securely encrypted.

(6) Use of CLETS for sending administrative messages is authorized for communications related to official business only.

(1) The DMV mails the renewal package to the appropriate command 90 days in advance of the expiration date to allow ample response time and/or to resolve any problems that may affect access to DMV data. The package consists of two copies of an Application/Agreement and an Employee Security Statement.

(2) Upon receipt from the DMV, each command shall provide the CHP CLETS Administrator the following information:

(a) Area Location Code.

(b) Department of Motor Vehicles Requester Code.

(c) Date of account expiration.

(3) Upon receipt of the above information, the CHP CLETS Administrator will forward a package containing instructions for the completion of this application.

(4) Commands are to ensure the application is completed according to the instructions provided by the CHP CLETS Administrator. Complete, sign, retain a copy for administrative file, and return both copies of the Application/Agreement to DMV. As this process only occurs once every four years, offices are to ensure the most recent copy is not purged, but always maintained in a current administrative file.

(5) Completion of the Employee Security Statement is not required as the CHP 101 takes its place.

e. Record Maintenance.

(1) Policy. Agencies that enter records into CLETS and/or NCIC must abide by CLETS/NCIC record maintenance policy. If a record has been properly maintained and the master case record (MCR) reflects the information on the record maintenance, then the record is to be judged as a good record in the system. Agencies are required to remove records that do not meet record maintenance requirements.

(2) Master Case Record. All records contributed to both CLETS and/or CJIS must be backed by an MCR (e.g., crime report or warrant). The MCR must contain complete information and be available at all times. The MCR must be stored at the location for the ORI that owns the record. In reference to Private Property Tows (PPTOW), the entry into CLETS shall only be made upon receipt of a written request by the tow company (i.e., facsimile). All PPTOW records shall immediately be provided to the appropriate Area office and shall be stored at the communications centers for no less than six months. Master case records stored electronically are acceptable if the records are readily accessible for hit confirmation and validation and meet all other record maintenance requirements. Whenever information is received which would change the data and/or status of the CJIS and/or NCIC record, the original record, as well as the CLETS Electronic Record Tracking (CERT), must be updated as soon as possible.

(3) California Law Enforcement Telecommunications Systems Electronic Record Tracking Application. The MCR must be accessible to communications and dispatch centers, Divisions, Areas, and CVEF offices, for the various tasks associated with the record. However, the MCR can reside in only one location.

Because of this, CHP has developed the CERT application. The CERT provides electronic information from the MCR, making it available to all CHP locations. The use of CERT will ensure CHP compliance with FBI and DOJ mandates. Commanders shall ensure CERT is utilized for any and all records entered into CLETS.

(a) Communications and dispatch centers shall use CERT for all records entered into CLETS or NCIC, to include:

1 Complete the initial entry into CERT. All fields shall be completed where information is available.

2 Update CERT with any additional information provided.

3 Update CERT with the File Control Number (FCN).

4 Reference and update CERT when responding to any hit confirmation request.

5 Update CERT for recovered stolen/lost vehicles/property.

(b) Division, Area, and CVEF offices shall use CERT for any record assigned to their location, including:

1 Conduct the second party accuracy check.

2 Update CERT with additional information from the MCR.

3 Conduct the NCIC validation.

4 Update the MCR, as needed.

5 Update CERT for recovered stolen/lost vehicles/property.

(c) Evidence officers and staff shall use CERT for all CLETS records they are responsible for, to include:

1 Complete the initial entry into CERT. All fields shall be completed where information is available.

2 Update CERT with any additional information provided.

3 Update CERT with the FCN.

4 Update CERT when any CLETS records are removed.

5 Conduct the second party accuracy check.

6 Conduct the NCIC validation.

(d) California Law Enforcement Telecommunications Systems Electronic Record Tracking-Assigned Numbers. The CERT application automatically generates a reference number upon initial creation of a CERT record. This number shall be entered in the Originating Case Number (OCA) field of the CLETS entry. The CAD log numbers shall be entered in the Miscellaneous field.

1 S Number. The Stolen Vehicle section is used for stolen vehicles, boats, plates, parts, and felony vehicle entries into SVS.

a The CERT automatically generates a stolen number (S number).

b The S number shall be used in the OCA field in the CLETS entry.

2 V Number. The Other Vehicle section is for stored, impounded, found, evidence, lost, pawned, repossessed vehicle, and boat entries made in SVS and ABS, as well as for allied agency recoveries.

a The CERT automatically generates a vehicle number (V number).

b The V number shall be used in the OCA field in the CLETS entry.

3 I Number. The Property section is for all property and firearm entries made in APS and AFS, and securities entries into NCIC.

a The CERT automatically generates an item number (I number).

b The I number shall be used in the OCA field in the CLETS entry.

4 P Number. The Persons section is for wanted, missing, and unidentified persons in WPS and MUPS, as well as for protected and restrained persons in the CARPOS.

a The CERT automatically generates a person number (P number).

b The P number shall be used in the OCA field in the CLETS entry.

(4) Second Party Accuracy Checks. To ensure the accuracy and completeness of CLETS and NCIC records, all entries shall be double-checked by a second party. This check shall be completed within seven calendar days and include ensuring the available cross-checks (e.g., DMV, Dealer's Record of Sales) were made and data in the CLETS record matches the data in the paper MCR. Since the MCR is located in the Division, Area, and CVEF offices, the second party accuracy check shall be performed by personnel from the same Area. Once the second party check has been completed, documentation into both the MCR and CERT shall be completed. The MCR shall be updated with who completed the second party check and the date.

(5) National Crime Information Center Record Validation.

(a) Policies from NCIC and CLETS require automated records in selected files be validated periodically by the contributors. The purpose of validation is to ensure the automated records are accurate, complete, and represent an active case. Inaccurate or invalid records (e.g., not an active case) may result in inappropriate action being taken against an innocent person or may jeopardize a peace officer's safety. (Refer to General Order [GO] 7.1, Validation Process for the National Crime Information Center Report, for specific validation procedures.)

(b) Vehicle and boat records are validated 60-90 days after entry, then annually. Other files have their records validated annually, based on month of entry.

(c) Validation is accomplished by reviewing the original entry and current supporting documents, and by recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicles registry files, or other appropriate source or individual. Consultation attempts are not mandatory for gun and securities records.

(d) In the event repeated attempts to contact the victim, complainant, etc., are unsuccessful, the location owning the record must determine, based on the best information and knowledge available, whether to retain the original record entry in the file.

(e) Both the MCR and CERT shall be updated with documentation of this validation, to include who completed the validation, the date, how contact was attempted or made, and the outcome of the contact.

(6) Hit Confirmations. Policy from NCIC/CLETS exists for both the owner of a CLETS record and for the agency that queries this CLETS record.

(a) When inquiries into SVS, ABS, WPS, AFS, APS, or MUPS result in a positive match (i.e., a hit) on a record, the inquirer must immediately confirm the hit with the originating agency. This ensures the validity of the hit before an arrest or seizure is made, thereby minimizing the potential for a false arrest and agency liability. The request for verification of a record is called a "Hit Confirmation Request" (YQ) and shall use the YQ message format (telephone contact can be made in addition to the YQ message being sent).

(b) The responsibility of the agency that entered the record is to be able to respond to the inquiring agency within ten minutes by checking the paper or electronic MCR. Running the record in CLETS is not acceptable verification of the record's validity, and shall not be done for this purpose. The actual confirmation as to the validity of the record from the record owner is called a "Hit Confirmation Response" (YR) and shall use the YR message format. An administrative message of confirmation without using the YQ/YR formats does not fulfill the criteria for hit confirmations through CLETS or NLETS.

(c) As record owners, CHP must be able to make a substantive response to hit confirmations within a ten-minute period, 24 hours a day, seven days a week. The substantive response would be one of the following:

1 The subject/item of inquiry is probably the same as the subject/item of the active record. Hit confirmed.

2 The subject/item of the inquiry is probably not the same as the subject/item of the active record. Hit denied.

3 This agency cannot confirm or deny the hit at this time. A hit confirmation will be provided (specify the time necessary to give notice; not to exceed two hours).

(d) The intent of the hit confirmation process is to provide the agency or officer with prompt information to make a decision in the field about whether to continue detaining the subject and/or confiscate the property.

(e) Dispatch personnel shall document all hit confirmation requests in CERT, regardless of whether a LOCATE is subsequently received.

1 Documentation should include the date and the name of the agency making the hit confirmation request and should be entered in the Miscellaneous box on the Entry tab in CERT.

(f) Failure to respond within the designated time (Priority U=Urgent, ten minutes; Priority R=Routine, one hour) may result in:

1 The DOJ initiating appropriate action to ensure proper response and compliance with system standards and procedures are followed in the future; and/or

2 Cancellation of the unconfirmed record by DOJ.

(g) Repeated failure to respond to hit confirmation requests may result in curtailment of CLETS, CJIS, or NCIC service, and revocation of entry/update capability.

(7) Locate Responsibility. When an inquiry to a CLETS record results in a match (i.e., a hit), the hit confirmation is positive, and the inquirer has probable cause to believe they are the same, the inquiring agency must place a LOCATE on the record. This is the only correct reason for placing a LOCATE. The LOCATE signifies property has been recovered or a wanted person apprehended. Under certain circumstances, failure to enter a LOCATE transaction could have legal liabilities.

(8) Recovered Property and Wanted Person Apprehensions. When a LOCATE is placed on a CLETS record, the contributor of the record must promptly CLEAR or CANCEL the record. The correct placement of a LOCATE on a record discharges DOJ's responsibility to include the record in its databases. If a record is in LOCATE status, and the contributor does not CLEAR or CANCEL the record in a timely manner, DOJ may CLEAR or CANCEL the record without the permission of the contributor.

5. TRAINING.

a. Training Requirements. The Department is required to participate in the CLETS/NCIC training program, as mandated by the FBI and DOJ. This training ensures all personnel (including youth aids, students, annuitants, consultants, or other nonpermanent staff) who handle or have access to CLETS records or the CLETS system are trained and certified in CLETS operation, policies, and procedures. Mandatory training shall be completed by all CHP employees, as well as non-CHP personnel with operator access to CLETS on CHP devices. Noncompliance will result in increased departmental liability, individual employee liability, and the potential loss of access to CLETS/NCIC systems. Additionally,

users with operator access will have their access removed if training is not up-to-date (to include WebWS, CAD, and mobile accounts). Specifically, DOJ requires the following:

(1) Provide initial training, functionally test, and affirm the proficiency of operators (Full Access/Less than Full Access). Provide appropriate basic training in CLETS/NCIC system use, policies, and regulations to nonoperator Practitioner (PRC) personnel.

(2) Biennially, provide functional retesting and reaffirm the proficiency of operators.

(3) Maintain records of all training, testing, and proficiency affirmation, including individual records for Full Access Operators (FAO).

(4) Provide continuing access to information concerning CLETS/NCIC systems for all personnel.

(5) Provide CLETS/NCIC training on system use, regulations, policies, audits, sanctions, and related civil liability for administrators and upper-level managers.

b. Training Levels and Requirements. The DOJ has identified four user levels of CLETS to be used for purposes of determining appropriate CLETS training. These levels, along with their respective training requirements, include:

(1) Full Access Operator. An FAO is any operator with the ability to make CLETS entries and/or updates, as well as inquiries into any of the CLETS/NCIC databases. This level will most often apply to communications centers personnel, evidence officers, and other personnel that would enter and/or update CLETS records. Training requirements include:

(a) Initial CLETS training.

(b) Review and acknowledgement of the CHP 101 (equivalent to the DOJ Employee Statement form).

(c) Completion of the FAO Telecommunications Workbook and exam (with a score of 70 percent or higher).

(d) A recertification exam shall be completed every two years (with a score of 70 percent or higher).

(e) Timely access to DOJ Information Bulletins, CLETS and NCIC manuals, and updates (available on the CHP Intranet site, under Resources, Technology, CLETS).

(2) Less Than Full Access Operator. A Less Than Full Access Operator (LFA) is an operator that makes inquiries only (no entries) into any of the CLETS/NCIC databases. This level will apply to any personnel that need to run their own CLETS inquires, including officers, sergeants, motor carrier specialists, designated clerical staff, and various administrative personnel. Training requirements include:

(a) Initial CLETS training.

(b) Review and acknowledgement of the CHP 101 (equivalent to the DOJ Employee Statement form).

(c) Completion of the LFA Telecommunications Workbook and exam (with a score of 70 percent or higher).

(d) A recertification exam shall be completed every two years (with a score of 70 percent or higher).

(e) Timely access to DOJ Information Bulletins, CLETS and NCIC manuals, and updates (available on the CHP Intranet site, under Resources, Technology, CLETS).

(3) Practitioner. Practitioner level training applies to employees who DO NOT have the ability to make their own inquiries into CLETS but have physical access to the information. Since anyone in CHP facilities has physical access, this level would apply to most nonoperators, including janitors, computer technicians, maintenance workers, and other office classifications. Training requirements include:

(a) Initial CLETS training, which consists of the discussion of both departmental and DOJ policies and procedures regarding CLETS/NCIC systems, security, and records.

(b) Review and acknowledgement of the CHP 101 (equivalent to the DOJ Employee Statement form).

(c) Timely access to DOJ Information Bulletins, CLETS and NCIC manuals, and updates (available on the CHP Intranet site, under Resources, Technology, CLETS).

(d) Recertification at this level consists of reacknowledging the CHP 101 every two years.

(4) Administrator. The Administrator level training applies to lieutenants and above and nonuniformed second-line supervisors and above. The DOJ requires Administrators complete the appropriate training according to the three training levels listed above (FAO, LFA, or PRC). Due to this dual classification, CHP has split the Administrator level into three specific training levels.

(a) Administrator 1. This level is to be used for someone that meets the criteria for the PRC level (non-CLETS operator) but is also a lieutenant and above or a nonuniformed second-line supervisor and above. Training requirements include:

1 Initial CLETS training, which consists of the discussion of both departmental and DOJ policies and procedures regarding CLETS/NCIC systems, security, and records.

2 Review and acknowledgement of the CHP 101 (equivalent to the DOJ Employee Statement form).

3 Review and acknowledgement of the NCIC "Areas of Liability for the Criminal Justice Information System Administrator" packet (also referred to as the NCIC Administrator packet).

4 Timely access to DOJ Information Bulletins, CLETS and NCIC manuals, and updates (available on the CHP Intranet site, under Resources, Technology, CLETS).

5 Recertification at this level consists of reacknowledging the CHP 101 and NCIC Administrator packet every two years.

(b) Administrator 2. This level is to be used for someone that meets the criteria for the LFA level (inquiry-only operator) but is also a lieutenant and above or a nonuniformed second-line supervisor and above. Training requirements include:

1 Initial CLETS training.

2 Review and acknowledgement of the CHP 101 (equivalent to the DOJ Employee Statement form).

3 Review and acknowledgement of the NCIC Administrator packet.

4 Completion of the LFA Telecommunications Workbook and exam (with a score of 70 percent or higher).

5 A recertification exam shall be completed every two years (with a score of 70 percent or higher).

6 Timely access to DOJ Information Bulletins, CLETS and NCIC manuals, and updates (available on the CHP Intranet site, under Resources, Technology, CLETS).

(c) Administrator 3. This level is to be used for someone that meets the criteria for the FAO level (CLETS record entry operator) but is also a lieutenant and above or a nonuniformed second-line supervisor and above. This level may only apply to Public Safety Dispatch Supervisor II level employees. Training requirements include:

1 Initial CLETS training.

2 Review and acknowledgement of the CHP 101 (equivalent to the DOJ Employee Statement form).

3 Review and acknowledgement of the NCIC Administrator packet.

4 Completion of the FAO Telecommunications Workbook and exam (with a score of 70 percent or higher).

5 A recertification exam shall be completed every two years (with a score of 70 percent or higher).

6 Timely access to DOJ Information Bulletins, CLETS and NCIC manuals, and updates (available on the CHP Intranet site, under Resources, Technology, CLETS).

c. California Law Enforcement Telecommunications System Training and Recordkeeping System. The CHP has developed an application called CTARS, which provides the only avenue for employees to complete their CLETS/NCIC training and testing online. The CTARS also maintains all records related to CLETS/NCIC training and testing. This online training is available to all personnel that have been issued a CHP network account. The CTARS can be accessed at http://ctars.chp.ca.gov.

(1) Once a user's network account has been set up, their training level can be assigned by the Area CLETS Coordinator.

(a) Upon user login to CTARS, the appropriate training videos, workbooks (if applicable), and exam (if applicable) will automatically be provided to the user. The user will be required to complete the tasks in a specific order.

(b) Upon completion of all tasks, the user will be advised of their score, and if the score is passing. If the score is passing, they will be advised their training is complete.

(c) If the user does not initially pass their exam, they can retake the exam as often as they like until a passing score is obtained. All records of nonpassing scores are then removed from the user's record.

(2) Biennially, all users will need to access CTARS to recertify their training level requirements. Users can complete the recertification process up to 90 days prior to their due date.

(3) Commanders are to access the CTARS Administrative page (http://ctarsadmin.chp.ca.gov) periodically to ensure all training is up to date.

d. Certified Instructors. With the implementation of CTARS, individual training classes are not required to be provided. However, if class instruction is preferred, only instructors who are certified by DOJ can provide the required CLETS/NCIC training.

(1) Only DOJ can certify instructors. The DOJ-provided training for trainers (T4T) is a 16-hour class held at various locations on various dates throughout the state. Contact the CHP CLETS Administrator to schedule instructors to attend the free T4T classes.

(2) Each instructor is required to self-certify every two years by taking the appropriate examination and logging the results on a separate roster. The instructor shall forward a copy of the results to CCSS, to the attention of the CHP CLETS Administrator.

(3) The workbook and exam cannot be completed in the classroom environment; both must be completed in CTARS.

e. Area Coordinators. Up to three individuals from each location code are to be designated as that Area's CLETS Coordinators, who will serve as liaisons with the CHP CLETS Administrator. The Area Coordinators are responsible for assigning new employees a CLETS training level and for coordinating and monitoring the status of online CLETS training for all employees.

f. System Updates. Employees have access to up-to-date information on new CLETS/NCIC systems and enhancements, CLETS/NCIC policy, and DOJ Information Bulletins, all located within the CLETS section on the CHP Intranet site.

6. ENFORCEMENT.

a. Sanctions.

(1) Any employee who is responsible for misuse of CLETS automated information is subject to adverse action. The Department will take appropriate action, which may include dismissal and submission of any criminal evidence to the local district attorney.

(2) Violations may also result in civil action against the employee, an employee's supervisor, and/or the Department.

(3) When accessing CLETS, any violation of law or CLETS rules, regulations, or operating procedures may result in action against the Department. In accordance with the DOJ's CLETS PPP, Section 1.10.1.B, sanctions could include a letter of censure, suspension of service, or removal of CLETS service.

b. Investigations.

(1) The DOJ mandates all agencies provide a detailed annual report of any investigations into the misuse of CLETS. This includes inquiries or investigations made into an employee's CLETS use, even if there are no findings of misuse. The CHP CLETS Support is required to submit one report to DOJ for all CHP locations. Due to DOJ reporting requirement, all CHP locations shall provide required information on CLETS misuse investigations to CHP CLETS Support when requested.

(a) For the purposes of reporting, if any action was taken to review any staff's use of CLETS, the DOJ has determined this to be an investigation (e.g., review of CAD logs, paper logs, search of CHP's journal), even if there are not findings of misuse. All locations shall include these instances when reporting CLETS misuse investigations to CHP CLETS Support. The investigations do not have to be considered "formal" to be counted.

(2) All identified instances of unauthorized disclosure, access, loss, or misuse of CLETS data shall also be reported to the Information Security Office (ISO) in IMD.

(3) Contact the ISO for assistance when an investigation is necessary due to a breach in system security. Commands are not to request assistance directly from DOJ.

(4) The Department monitors all CLETS transactions from CHP systems, which can be identified by terminal mnemonic, employee ID number, date, and time. The DOJ monitors all CLETS transactions statewide and can search individual files to identify any inquiries.

c. Audits.

(1) The DOJ conducts CLETS-related audits and/or site inspections on a triennial basis. The FBI also conducts triennial audits of DOJ and a select number of local agencies. When notified of any audit or audit results, commanders shall contact the CHP CLETS Administrator, who will assist with the audit completion. The three types of audits are described below.

(2) California Law Enforcement Telecommunications System Policy and Security Audit. This audit will often include a site inspection, and focuses on the following areas:

(a) Fingerprinting. The CHP CLETS policy requires the submission of a fingerprint check to the DOJ and FBI for all personnel with unescorted physical access to facilities where CLETS-provided information, both on terminal screens and printed records, can be viewed. This includes access by volunteers, contract personnel, and other nondepartmental personnel.

(b) California Law Enforcement Telecommunications System Training and Records. The CHP CLETS/NCIC initial and recertification training is required for all CHP personnel. The CHP CLETS training records are kept in the CTARS. (Refer to paragraph 5 of this chapter.)

(c) Information Security and Privacy Protection Training. Each location will need to produce the Information Security and Privacy Protection training records for all personnel.

(d) Confirmation of Stolen Vehicles. The DOJ and FBI policies require stolen vehicle hits be confirmed through the MCR rather than through SVS. This does not preclude communications centers from immediately advising officers of the SVS hit. However, all hits on stolen or wanted vehicles will be verified by immediately contacting the agency owning the record. Likewise, when requested by an outside agency, CHP shall access CERT prior to advising if the record (or hit) is a good record.

1 The MCR shall be accessed for the hit confirmation. Since the MCR is not available to dispatch personnel, CERT must be accessed for this verification.

2 The DOJ has determined if the CERT record is not updated with all available information (from the CHP 180, Vehicle Report, etc.), then they consider the Department to not have access to the MCR for the purpose of hit confirmation and will find the CHP location out of compliance.

(3) The Criminal Offender Record Information Audit. The CORI audit the location's use of criminal history information.

(a) The auditors will pull various records run by the Area's ORI and request substantiating documentation for the records (to show the inquiry meets both the right-to-know and need-to-know mandates of DOJ Policies, Practices and Procedures [and Statues], Section 1.6.4, Confidentiality of Information from the CLETS).

(b) The auditors will pull various records run by the Area's ORI and check the RETURN TO OFFICER/DIVISION field (in WebWS) and RETURN TO or RTE fields (in CAD) to ensure the appropriate information was included. (Refer to paragraph 3.a.(3) of this chapter for further information.)

(c) Each location will be asked if all inquiries made into CHS are tracked/documented, and/or if all releases of criminal history information outside of the Department are tracked/documented.

(4) The California Law Enforcement Telecommunications System Database Audit. This audit looks at the CLETS entries made; the documentation and record maintenance performed on the entries.

(a) All entries into CLETS must be supported by a paper MCR, in addition to a CERT record (e.g., found license plates, storages, PPTOW).

(b) If a record is in CLETS (e.g., vehicle, plates, firearms, property), the paper MCR must be available at the office location.

(c) The CERT records shall contain as much information from the MCR as possible.

(d) Firearms entries for stolen, lost, and found firearms shall be entered as Entry Level 2.

(e) Documentation. Retain DMV printouts of vehicles entered into the SVS with the case file.

(f) Multiple System Entries. Frequently, a single incident will result in multiple system entries. For example, a report taken on a stolen vehicle containing a stolen weapon will have entries in both SVS and AFS. If the vehicle is recovered, it must be cleared from SVS, but the MCR must be retained as long as the weapon remains in AFS. To ensure the file is not inadvertently purged, a copy of the report shall be made and kept for the additional entry in CLETS.

(g) Data Verification. Second party accuracy checks of entry information must be completed on all records entered into CLETS by a second party. This ensures the information in the system matches the data in the MCR, refer to paragraph 4.e.(4) of this chapter for additional information.

(h) National Crime Information Center Validation. All requests for validation shall be completed. Contact with the reporting party shall be attempted for all records (except guns and securities), to determine if the record is still outstanding. Refer to GO 7.1 and paragraph 4.e.(5) of this chapter for further validation procedures. Maintain documentation of validation attempts and responses in the case file, as well as in the CERT record.

(i) Data Entry Errors. Following are three frequent data entry errors which must be avoided:

1 The OCA must contain information to locate the actual case. A CERT record is required for all CLETS entries, users shall use the CERT assigned number in the OCA field.

2 Do not use a communications center's ORI for any CLETS entry, as the ORI field should indicate where the paper file is located.

3 Do not substitute DMV codes for CJIS/NCIC codes for vehicle/vessel model and body.

(5) Areas should designate an individual to assist DOJ representatives when conducting a CLETS audit or inspection. The selected individual should be familiar with CLETS, CLETS audit paperwork, the location of all CLETS terminals, and training records.

THIS PAGE INTENTIONALLY LEFT BLANK