

California
Law
Enforcement
Telecommunications
System

Policies,
Practices and
Procedures
(and Statutes)



C A L I F O R N I A

DEPARTMENT OF JUSTICE

CLETS POLICIES, PRACTICES and PROCEDURES

Table of Contents

	SUMMARY OF CHANGES	5
1.0	LEGISLATIVE INTENT AND LAW	6
1.01	California Government Code – Chapter 2.5	6
1.1	PURPOSE AND SYSTEM DESCRIPTION	11
1.1.1	Purpose of the CLETS	11
1.1.2	State-Provided Services	11
1.1.3	Request for General Information	11
1.2	THE CLETS ADVISORY COMMITTEE	12
1.2.1	Responsibilities of Committee.....	12
1.2.2	Subcommittees.....	12
1.2.3	Committee Member Consultation.....	12
1.2.4	CLETS Advisory Committee Meetings.....	12
1.3	QUALIFICATIONS FOR MEMBERSHIP IN THE CLETS	13
1.3.1	Eligibility for CLETS Service	13
1.3.2	Security Requirements.....	14
1.3.3	Applicant Request for Service	14
1.3.4	Subscriber Agreement	14
1.3.5	Agency CLETS Coordinator	15
1.3.6	Security Point of Contact.....	15
1.4	THE CLETS INTERFACES	16
1.4.1	Connections	16
1.4.2	Requirements for all Law Enforcement and Criminal Justice Agencies.....	16
1.4.3	Requirements for Both County Control Agency and Direct Interface System Host...16	
1.4.4	County Control Agency.....	18
1.4.5	Direct Interface System Host.....	19
1.4.6	Local Agency Direct Interface.....	20
1.4.7	Local Agency Petitioning to Terminate Access through a Direct Interface or a Direct Interface System Host.....	21
1.4.8	Removal of County Control Agency/Direct Interface System Host	21
1.5	CONTRACTUAL AGREEMENTS.....	22
1.5.1	Management Control Agreement	22
1.5.2	Interagency Agreement for Placement of a CLETS Terminal	24
1.5.3	Release of Information from the CLETS	25
1.5.4	Reciprocity Agreement.....	25

1.5.5	Interstate Access	26
1.6	SYSTEM RULES	26
1.6.1	Database Policies and Regulations	26
1.6.2	Terminal Mnemonics.....	28
1.6.3	Audits and Inspections.....	30
1.6.4	Confidentiality of Information from the CLETS.....	30
1.6.5	Administrative Messages.....	30
1.6.6	Local/Wide Area Networks – Definition and Requirements.....	30
1.6.7	Operator Identification Field (OIF) Requirements	31
1.6.8	Terminal Address Field (TAF) Requirements	32
1.7	SYSTEM DESIGN AND ENHANCEMENT STANDARDS	33
1.7.1	Message Switching Computer (MSC) Definition and Requirements.....	33
1.7.2	MSC Design	33
1.7.3	System Upgrade.....	33
1.7.4	MSC Test Lines	34
1.8	TRAINING	34
1.8.1	System Training.....	34
1.8.2	Database Training.....	35
1.8.3	Security Awareness Training.....	36
1.9	OPERATIONAL CONTROL, OVERSIGHT and COMPLIANCE RESPONSIBILITY	37
1.9.1	Information Technology (IT) Security Incident Response Reporting.....	37
1.9.2	Background and Fingerprint-Based Criminal Offender Record Information Search..	37
1.9.3	User Access	38
1.9.4	Non-Federal, Non-State, and Non-Local Governmental Employees	39
1.9.5	System Use Notification Recommendation.....	39
1.10	SYSTEM DISCIPLINE/APPEAL PROCESS	40
1.10.1	System Misuse.....	40
1.10.2	Discontinuance of CLETS Service.....	42
	GLOSSARY	44

Exhibits

Exhibits listed below are forms available on the California Law Enforcement Web (CLEW) portal.
<https://clew.doj.ca.gov/forms>

- Exhibit A [HDC 0001 CLETS Subscriber Agreement](#)
- Exhibit B [HDC 0002 Change Request](#)
- Exhibit C [HDC 0003 ACC Responsibilities](#)
- Exhibit D1 [HDC 0004A Management Control Agreement](#)
- Exhibit D2 [HDC 0004B Private Contractor Management Control Agreement](#)
- Exhibit E [HDC 0005 Interagency Agreement](#)
- Exhibit F [HDC 0006 Release of Information from the CLETS](#)
- Exhibit G [HDC 0007 Reciprocity Agreement](#)
- Exhibit H [HDC 0008 MSC/Users Costs and Requirements](#)
- Exhibit I [HDC 0009 Employee/Volunteer Statement Form](#)
- Exhibit J [HDC 0010 CLETS Misuse Investigation Reporting Form](#)
- Exhibit K [HDC 0011 CA DOJ Security Point of Contact Delineation and Agreement](#)
- Exhibit L [HDC 0017 CLETS IT Security Incident Response Form](#)

SUMMARY OF CHANGES

This document reflects changes to the December 2019 version of the California Law Enforcement Telecommunication System (CLETS), Policies, Practices and Procedures (PPP). The California Department of Justice (DOJ)-approved changes are italicized below:

- 1.01 This is a new section of the Government Code related to Assembly Bill 44 and tribal law enforcement/court CLETS access.*
- 1.3.1. A and 1.3.1.B These sections were modified to include qualifying tribal agencies to the definitions of Class I law enforcement subscribers and Class II criminal justice agencies. Additionally, “sub-unit” language was added to section 1.3.1.B to further clarify that eligible sub-units of public agencies that perform a criminal justice function other than apprehension may be eligible for CLETS access.*
- 1.5.1.A This section was modified to provide additional clarification that Management Control Agreements must not only be received by DOJ, but also approved by DOJ. This section was also modified to include tribal law enforcement agencies and tribal courts as agencies that are required to submit Management Control Agreements when applicable.*
- 1.5.4 This section was modified to provide additional clarification that Reciprocity Agreements must not only be received by DOJ, but also approved by DOJ.*
- 1.8.2.A.1 This section was modified to be consistent with the updates to FBI Criminal Justice Information Services (CJIS) Security Policy, section 5.2 “Awareness and Training (AT),” subsection AT-2.*
- 1.8.2.A.2 This section was modified to be consistent with the updates to FBI CJIS Security Policy, section 5.2 “Awareness and Training (AT),” subsection AT-2.*
- 1.8.2.A.3 This section was modified to be consistent with the updates to FBI CJIS Security Policy, section 5.2 “Awareness and Training (AT),” subsection AT-4.*
- 1.8.2.A.4 This section was modified to be consistent with the updates to FBI CJIS Security Policy, section 5.2 “Awareness and Training (AT),” subsection AT-2.*
- 1.9.1 This section was modified to include language that reflects the current practice of contacting the 24/7 DOJ Computer Operations unit.*
- 1.9.2.A This section was modified to provide additional clarification regarding the fingerprint-based state and federal level background checks required for all persons with physical or logical access to CLETS.*
- 1.9.4 This section was modified to include tribal law enforcement agencies as agencies that are required to submit certification and/or deputization agreements when applying for CLETS access, when applicable.*
- Glossary This section was modified to add a definition of Tribe.*

1.0 LEGISLATIVE INTENT AND LAW

1.01 California Government Code – Chapter 2.5

California Government Code (GC) sections 15150 through 15167 state that the California Department of Justice (DOJ) shall maintain a statewide telecommunications system for the use of law enforcement agencies. Chapter 2.5 is quoted as follows:

CHAPTER 2.5 CALIFORNIA LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM (CHAPTER 2.5 added by Stats. 1965, Ch. 1595)

15150. (a) It is the intent of the Legislature that the Department of Justice shall commence to operate under this chapter as soon as feasible, but until such time, the department shall continue to operate under Article 8 (commencing with § 13240) of Chapter 2, Part 3, Division 3, Title 2 of this code, and Chapter 2 (commencing with § 15100) of this part. Accordingly, the department shall not discontinue service to any connection point to which it is required to furnish services at state expense until it has made the determination, has given notice, and the notice period has elapsed, as provided in subdivision (b).

(b) At such time as the Attorney General concludes that he can furnish service to one location in any county in compliance with the requirements of § 15161, he shall so certify and shall send notice of such certification to each agency in the county connected with the state system. Thirty days after the sending of such notice, service to any connection point in the county other than the one location selected pursuant to § 15161 shall no longer be at state expense. (Added by Stats. 1965, Ch. 1595.)

15151. The maintenance of law and order is, and always has been, a primary function of government and is so recognized in both Federal and State Constitutions. The state has an unmistakable responsibility to give full support to all public agencies of law enforcement. This responsibility includes the provision of an efficient law enforcement communications network available to all such agencies. It is the intent of the Legislature that such a network be established and maintained in a condition adequate to the needs of law enforcement. It is the purpose of this chapter to establish a law enforcement telecommunications System for the State of California. (Added by Stats. 1965, Ch. 1595)

15152. The Department of Justice shall maintain a statewide telecommunications system of communication for the use of law enforcement agencies. (Added by Stats. 1965, Ch. 1595)

15153. The system shall be under the direction of the Attorney General, and shall be used exclusively for the official business of the state, and the official business of any city, county, city and county, or other public agency. (Added by Stats. 1965, Ch. 1595.)

15154. The Attorney General shall appoint an advisory committee of the California Law Enforcement Telecommunications System, hereinafter referred to as the committee, to advise and assist him in the management of the system with respect to operating policies, service evaluation, and system discipline. The committee shall serve at the pleasure of the Attorney General without compensation except for reimbursement of necessary travel expenses.

Before requesting vendor proposals to implement the system, the committee shall prepare detailed technical system specifications defining all communications – handling parameters and making explicit in sufficient depth the goals of the system. (Added by Stats. 1965, Ch. 1595.)

15155. *The committee shall consist of representation of the following organizations:*

- (1) Two representatives from the Peace Officers' Association of the State of California.*
 - (2) One representative from the California State Sheriffs' Association.*
 - (3) One representative from the League of California Cities.*
 - (4) One representative from the County Supervisors Association of California.*
 - (5) One representative from the Department of Justice.*
 - (6) One representative from the Department of Motor Vehicles.*
 - (7) One representative from the Office of Emergency Services.*
 - (8) One representative from the California Highway Patrol.*
 - (9) One representative from the California Police Chiefs Association.*
- (Added by Stats. 1965, Ch. 1595; amended by Stats. 2014, Ch. 54)*

15156. *The Department of Justice shall provide an executive secretary to the committee. (Added by Stats. 1965, Ch. 1595.)*

15157. *The committee shall elect a chairman for a term to be determined by the committee. (Added by Stats. 1965, Ch. 1595.)*

15158. *The committee shall meet at least twice each year at a time and place to be determined by the Attorney General and the chairman. Special meetings may be called by the Attorney General or the chairman by giving at least 14 days' notice to the members. (Added by Stats. 1965, Ch. 1595.)*

15159. *All meetings of the committee and all hearings held by the committee shall be open to the public. (Added by Stats. 1965, Ch. 1595.)*

15160. *(a) The Attorney General shall, upon the advice of the committee, adopt and publish for distribution to the system subscribers and other interested parties the operating policies, practices and procedures, and conditions of qualification for membership.*

(b) (1) Commencing on January 1, 2020, consistent with the California Values Act (Chapter 17.25 (commencing with Section 7284) of Division 7 of Title 1), no subscribers to the system shall use information other than criminal history information transmitted through the system for immigration enforcement purposes, as defined in subdivision (f) of Section 7284.4. In addition, no subscribers to the system shall use the system for purposes of investigating violations of Section 1325 of Title 8 of the United States Code, if a violation of that section is the only criminal history in an individual's record. This section does not prohibit or restrict any government entity or official from sending to, or receiving from, federal immigration authorities, information regarding the citizenship or immigration status, lawful or unlawful, of an individual, or from requesting from federal immigration authorities immigration status information, lawful or unlawful, of any individual, or maintaining or exchanging that information with any other federal, state, or local government entity, pursuant to Sections 1373 and 1644 of Title 8 of the United States Code.

(2) Commencing on July 1, 2021, any inquiry for information other than criminal history information submitted through the system shall include a reason for the initiation of the inquiry.

(3) Commencing on July 1, 2021, the Attorney General, and personnel they so authorize, may conduct investigations, including inspections and audits, as the Attorney General deems appropriate to monitor compliance with this subdivision. The Attorney General or authorized personnel who are conducting an investigation pursuant to this subdivision shall be authorized to review and inspect case files and any records identified in the investigation process to substantiate a reason given for accessing information other than criminal history information in the system.

(c) For the purposes of this section, "system" means the statewide telecommunications system of communication established pursuant to this chapter.

(Amended by Stats. 2019, Ch. 789, Sec. 1. (AB 1747))

15161. *The Department of Justice shall provide a basic telecommunications communications network consisting of no more than two relay or switching centers in the state and circuitry and terminal equipment in one location only in each county in the state. The system shall be consistent with the functional specifications contained in pages 75 to 79 of the Report of the Assembly Interim Committee on Ways and Means, Volume 21, Number 9, 1963-1965.*

These functional specifications summarize the needs of the peace officers for present purposes, but do not constitute technical specifications addressed to prospective suppliers of equipment and procedures.

(Added by Stats. 1965, Ch. 1595.)

15162. *The system may connect and exchange traffic with compatible systems of adjacent states and otherwise participate in interstate operations. (Added by Stats 1965, Ch. 1595.)*

15163. *The system shall provide service to any law enforcement agency qualified by the committee which, at its own expense, desires connection through the county terminal. (Added by Stats 1965, Ch. 1595.)*

15164. *The system shall be maintained at all times with equipment and facilities adequate to the needs of law enforcement. The committee shall recommend to the Attorney General any improvements of the system to meet the future requirements of the subscribers and to take advantage of advancements made in the science of telecommunications communications. The system shall be designed to accommodate present and future data processing equipment. (Added by Stats. 1965, Ch. 1595.)*

15164.1. *(a) The person designated as a county's "control agent" as defined by the policies, practices, and procedures adopted pursuant to § 15160, or the chief officer of any other agency that has been granted direct access to the California Law Enforcement Telecommunications System under the provisions of this chapter, shall have sole and exclusive authority to ensure that the county's or other agency's equipment connecting to the California Law Enforcement Telecommunications System complies with all security requirements that are conditions of access to the California Law Enforcement Telecommunications System under the provisions of this chapter, or the policies, practices, and procedures adopted pursuant to § 15160, and that the equipment complies with the county control agent's security policy. This authority shall include,*

but not be limited to, locating, managing, maintaining, and providing security for all of the county's or other agency's equipment that connects to, and exchanges data, video, or voice information with, the California Law Enforcement Telecommunications System under the provisions of this chapter, including, but not limited to, telecommunications transmission circuits, networking devices, computers, databases, and servers.

(b) A control agent or chief officer may not exercise the authority granted in subdivision (a) in a manner that conflicts with any other provision of this chapter, or with the policies, practices, and procedures adopted pursuant to § 15160. (Added by Stats. 2001, Ch. 34)

15165. *Any subscriber to the system shall file with the Attorney General an agreement to conform to the operating policies, practices and procedures approved by the committee under penalty of suspension of service or other appropriate discipline by the committee. (Added by Stats. 1965, Ch. 1595.)*

15166. *The Director of General Services shall fix the charge to be paid by any state department, officer, board or commission to the Department of Justice. (Added by Stats. 1965, Ch. 1595.)*

15167. *In the case of a state agency, the charge shall be paid from the money available by law for the support of the state agency using the system. (Added by Stats. 1965, Ch. 1595.)*

15168. *(a) Notwithstanding Section 15153, the system may connect and exchange traffic with the compatible systems of a tribal government, as provided in this section.*

(b) A law enforcement agency or court of a tribe may apply to the Attorney General for access to the system. The Attorney General shall provide system access to any law enforcement agency or court of a tribe that has made application and that meets all of the qualifications prescribed in subdivision (c), as determined by the Attorney General. System access provided to a tribe shall be at the sole expense of that tribe.

(c) The Attorney General shall deem a tribe that has applied for system access pursuant to subdivision (b) to be qualified only if the governing body of that tribe has enacted or adopted a law, resolution, or ordinance, which shall be maintained in continuous force, that provides for all of the following:

- (1) The tribe expressly waives its right to assert its sovereign immunity from suit, regulatory or administrative action, and enforcement of any ensuing judgment or arbitral award, for any and all claims arising from any actions or omissions of the tribe, including its officers, agents, and employees, when acting within the scope of their authority and duty, arising out of, connected with, or related to, the system.*
- (2) The tribe expressly agrees that the substantive and procedural laws of the State of California shall govern any claim, suit, or regulatory or administration action, that the obligations, rights, and remedies shall be determined in accordance with such laws, and that the courts of the State of California or of the federal government, as applicable, shall have exclusive jurisdiction.*
- (3) The tribe agrees to cooperate with any inspections, audits, and investigations by the Department of Justice for improper use or compliance with the operating policies, practices, and procedures, including any sanction or discipline imposed by the*

department, up to and including removal of system access.

- (4) The tribe and its agencies, entities, or arms, including any officers, agents, and employees of the tribe when acting within the scope of their authority and duty, shall comply with the laws of the State of California relating to the use of records and information from the system, including, without limitation, Section 6200 and this chapter, Sections 502, 11105, 11141, 11142, 11143, and 13300 to 13304, inclusive, of the Penal Code, and Section 1808.45 of the Vehicle Code.*
- (5) The tribe and its agencies, entities, or arms, including any officers, agents, and employees of the tribe when acting within the scope of their authority and duty, shall comply with the Department of Justice's regulations, agreements, and operating policies, practices, and procedures, relating to the security requirements, access to the records and information from the system, and use of records and information from the system.*

(d) The intent of the Legislature in enacting this section is to grant tribes access to, and use of, criminal justice databases, and the information in those databases, in a manner similar to the access granted under federal law codified in Section 534 of Title 28 of, and Section 41107 of Title 34 of, the United States Code.

(e) The Director of General Services shall determine the charges to be paid by a tribe to the department for system access, including any initial setup charges and any ongoing charges for access. These charges shall be reasonably similar to those imposed on other system subscribers.

(f) As used in this section, the following terms are defined as follows:

- (1) "Tribe" means a federally recognized Indian Tribe whose territorial boundaries lie wholly or partially within the State of California, and any agencies, entities, or arms of the tribe, as applicable, either together or separately.*
- (2) "Sovereign immunity" means immunity from suit or action of the tribe and its agencies, entities, or arms, including the officers, agents, and employees of the tribe when acting within the scope of their authority and duty. (Added by Stats. 2023, Ch. 638, Sec. 2. (AB 44))*

1.1 PURPOSE AND SYSTEM DESCRIPTION

1.1.1 Purpose of the CLETS

Pursuant to GC section 15151, the California Law Enforcement Telecommunications System (CLETS) is an efficient law enforcement communications network available to all public agencies of law enforcement within the state. The CLETS will provide all law enforcement and criminal justice user agencies with the capability to obtain information directly from federal and state computerized information files. For interstate access, see PPP section 1.5.5.

1.1.2 State-Provided Services

Pursuant to GC sections 15161 through 15163, DOJ shall provide central switching equipment and sufficient circuitry from the switching center to one location in each county to handle law enforcement message traffic. Circuitry and terminal equipment to extend beyond, or other than, the CLETS termination point in each county will be provided by client agencies at their own expense.

1.1.3 Request for General Information

Requests for information concerning the general administration of the CLETS or notification of changes and additions to system equipment and facilities that affect the CLETS should be directed to the:

CLETS Administration Section
Department of Justice
P.O. Box 903387
Sacramento, CA 94203-3870
Telephone: (916) 210-4240
Facsimile: (916) 227-0696
E-mail address: CAS@doj.ca.gov

Other helpful information, publications and forms can be found on the California Law Enforcement Web (CLEW) at <https://clew.doj.ca.gov>.

1.2 THE CLETS ADVISORY COMMITTEE

1.2.1 Responsibilities of Committee

The responsibilities of the CLETS Advisory Committee (CAC) are defined in GC sections 15154 through 15164.

1.2.2 Subcommittees

The chair of the CAC may appoint subcommittees and/or workgroups to consider the CLETS user qualifications, operating rules, policies and practices, and other matters as appropriate. These subcommittees may be either standing or ad hoc.

A Standing Strategic Planning Subcommittee (SSPS) shall be established to evaluate the legislative, user and technical environment of the CLETS to make timely recommendations to the CAC and perform or update planning functions or documents as directed by the CAC. The following work groups may be established under the direction of the SSPS: Administration, Technical and Legislation.

1.2.3 Committee Member Consultation

Under emergency conditions, the chair, through the CLETS Executive Secretary, may, without benefit of a formal committee meeting, consult individual committee members to expedite clarification of policy or procedure questions.

1.2.4 CAC Meetings

Pursuant to GC section 15158, the CAC shall meet at least twice each year. Alternates are not allowed for any member who is unable to attend a meeting.

1.3 QUALIFICATIONS FOR MEMBERSHIP IN THE CLETS

1.3.1 Eligibility for CLETS Service

GC section 15163 states, “The system shall provide service to any law enforcement agency qualified by the committee which, at its own expense, desires connection through the county terminal.” A public agency or sub-unit thereof that performs law enforcement or criminal justice functions pursuant to a statute, ordinance or regulation and to which it appropriates more than 50% of its annual budget may apply for the CLETS service. Participating agencies in the CLETS are referred to as a law enforcement agency, a criminal justice agency or a sub-unit of a public agency. A sub-unit is defined as a unit of a non-law enforcement public agency that performs the duties of a law enforcement agency, whose employees are peace officers, and the majority of whose annual budget (more than 50%) is allocated to the administration of criminal justice. Participating agencies in the CLETS are referred to as Class I-Law Enforcement, Class II-Criminal Justice or Class III-other types of law enforcement agencies as defined below.

- A. A Class I-law enforcement subscriber is defined as a public or tribal agency having statutory powers of arrest and whose primary function is that of apprehension and detection. Class I users include, but are not limited to, sheriffs, city police departments, tribal police departments, California Highway Patrol, Department of Justice, and the Federal Bureau of Investigation.
- B. A Class II-Criminal Justice agency is a public agency, tribe, or any sub-unit thereof, performing a criminal justice function other than apprehension. Class II subscribers include agencies devoted to the administration of criminal justice with personnel whose primary purpose is detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, rehabilitation of accused persons or criminal offenders, criminal identification activities, and the collection, storage and dissemination of criminal history record information. Agencies include, but are not limited to, district attorneys, courts, tribal courts, probation departments, and other miscellaneous local, state and federal agencies or sub-units thereof performing such functions.
- C. A Class III subscriber is the sub-unit of a non-law enforcement public agency which performs the duties of a law enforcement agency, and whose employees are peace officers. Examples of Class III agencies include the Department of Insurance - Fraud Division, the Employment Development Department - Investigations Bureau, university, college and school district police departments, and any fire department - arson investigation unit.

1.3.2 Security Requirements

All agencies applying for access to the CLETS must adhere to the requirements established in the PPP and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (CSP). If access is granted, it is each agency's responsibility to ensure, annually, that the requirements of the PPP and FBI CSP are reviewed to ensure the agency is still in compliance. System misuse must be reported to DOJ by February 1st of each year, for the prior calendar year, even if no misuse occurred.

The policies can be found on the CLEW at <https://clew.doj.ca.gov>.

1.3.3 Applicant Request for Service

Agencies desiring access to the CLETS must submit an application through the County Control Agency/Direct Interface System Host, if applicable (refer to section 1.4 for description of County Control Agency/Direct Interface System Host).

- A. All applications for new service and any upgrade application that results in a policy change or utilizes technology that has not previously been approved by the CAC will be brought before the CAC. These applications are considered non-routine.
- B. Routine applications are defined as upgrade applications that utilize technology previously approved by the CAC. These applications will be approved by DOJ. Any routine application with outstanding issues may be referred to the CAC on a case-by-case basis.

In the event a routine or non-routine application is denied, DOJ shall provide the applicant agency with a written notice specifying all causes for denial. The applicant agency may file, within 30 days from the date of the notice of denial, a written request with DOJ for reconsideration by the CAC. Such a request must include all arguments the applicant agency feels are relevant to a reconsideration of the application. DOJ shall present the written request for reconsideration to the CAC at the next regularly scheduled CAC meeting. The CAC shall make the final decision. DOJ shall provide the applicant agency with a written notice of the final decision.

1.3.4 Subscriber Agreement

All agencies participating in the CLETS must file a Subscriber Agreement signed by the agency head and submitted to DOJ as required by GC section 15165. A new Subscriber Agreement (reference Exhibit A) shall be updated when the head of the agency changes or immediately upon request from DOJ.

1.3.5 Agency CLETS Coordinator

Each CLETS subscribing agency must designate an Agency CLETS Coordinator (ACC) who serves as the coordinator with DOJ on matters pertaining to the use of the CLETS, the FBI National Crime Information Center (NCIC), the International Justice and Public Safety Network (Nlets) and DOJ criminal justice databases and administrative network that the CLETS accesses. The ACC will be responsible for ensuring compliance with DOJ/FBI policies and regulations including validation requirements, as well as facilitating the exchange of the CLETS administrative information between DOJ and the ACC's agency.

The ACC's responsibilities shall be designated by DOJ on an ACC Responsibilities Form (reference Exhibit C). If an agency requests to have someone other than a permanent, full-time employee as its ACC, DOJ must be notified in writing and will review the request. Any change in the ACC's designation must immediately be provided to DOJ on the Change Request Form (reference Exhibit B).

1.3.6 Security Point of Contact

Pursuant to the FBI CSP section 3.2.2.2e, each CLETS subscribing agency must designate a Local Agency Security Officer, hereinafter referred to as the Security Point of Contact (SPOC), who serves as the security coordinator with DOJ on security matters pertaining to the use of the CLETS, the NCIC, the Nlets and DOJ criminal justice databases and administrative network that the CLETS accesses. Any information communicated between DOJ and the SPOC will be shared with the agency's ACC.

The SPOC's responsibilities shall be designated by DOJ on a SPOC Responsibilities Form (reference Exhibit K). If an agency requests someone other than a permanent, full-time employee as its SPOC, DOJ must be notified in writing and will review the request. Any change in the SPOC's designation must immediately be provided to DOJ on the Change Request form (reference Exhibit B).

1.4 THE CLETS INTERFACES

1.4.1 Connections

A CLETS connection may be obtained via three types of interfaces:

- A. County Control Agency – Government Code (GC) section 15161 requires DOJ to provide a basic telecommunications network consisting of no more than two switching centers in the state and circuits/equipment to provide service to one location only in each county in the state. This single direct interface in each county is referred to as the County Control Agency.
- B. Direct Interface System Host – An agency other than the County Control Agency, opting to host the CLETS service for other subscribing agencies, is referred to as the Direct Interface System Host.
- C. Local Agency Direct Interface – An agency opting to interface directly to DOJ for the CLETS, and not host other agencies, is referred to as a Local Agency Direct Interface.
- D. The link between the above interfaces and DOJ is the responsibility of DOJ to manage, maintain and encrypt. Agencies that are utilizing the interfaces above are responsible for the integrity and security of the network segment that hosts the CLETS message switching computer (MSC). Pursuant to GC section 15164.1, the County Control Agent or chief officer of any other agency who has been granted direct access to the CLETS shall have sole and exclusive authority to ensure the equipment of the county or other agency connecting to the CLETS complies with all security requirements as required by the PPP.

1.4.2 Requirements for all Law Enforcement and Criminal Justice Agencies

All agencies accessing the CLETS, whether direct or indirect, are required to comply and adhere to the requirements established in PPP section 1.3.2. It is each agency's responsibility to ensure the requirements are reviewed annually to guarantee compliance.

1.4.3 Requirements for Both County Control Agency and Direct Interface System Host

A. Role and Responsibilities

The County Control Agency/Direct Interface System Host serves as the CLETS host agency and establishes the requirements for access through its MSC. It is the responsibility of the County Control Agency/Direct Interface System Host to review all new and upgraded applications to ensure compliance with PPP section 1.3.2 for agencies accessing the CLETS behind their respective MSC.

It is the responsibility of the host agency to inform its subscribing agencies of the following:

1. The type of circuitry and equipment necessary for access and how it can be obtained.
2. The type of services provided by the host MSC, in addition to the CLETS access, such as countywide databases or dispatching.

3. All fees that will be charged for the CLETS service, equipment rental, line costs and any additional services.

The County Control Agency/Direct Interface System Host is required to train its subscribing agencies on how to utilize the CLETS to access databases via the hosting MSC and how to use preformatted screens, if provided by the host system.

B. Mnemonics

The County Control Agency/Direct Interface System Host will request additional terminal mnemonics or changes to database authorizations for all subscribing agencies behind its system.

1. The subscribing agency must submit a completed "Terminal Access Request Form" to the County Control Agency/Direct Interface System Host.
2. The MSC administrator for the County Control Agency/Direct Interface System Host will review the request to ensure it can be accommodated by the MSC, sign the request and forward it to DOJ.
 - a. If the County Control Agency/Direct Interface System Host cannot accommodate the request, the subscribing agency has the following options:
 1. Wait until the County Control Agency/Direct Interface System Host can accommodate the request; or
 2. Seek access via other means as identified in PPP section 1.4.1.
 - b. In the event the County Control Agency/Direct Interface System Host continues to be unable to fulfill its responsibilities in providing access, it shall be the responsibility of DOJ, in consultation with the CLETS Advisory Committee (CAC), to seek immediate remedy in accordance with PPP section 1.4.7.

Upon completion of the CLETS terminal authorization changes, the CLETS Administration Section (CAS) will advise the MSC administrator, who will program the MSC for the additional terminals or authorization changes and notify the subscribing agency.

1.4.4 County Control Agency

A. Role and Responsibilities

Pursuant to GC section 15163, the CLETS service shall be provided to any law enforcement or criminal justice agency qualified by DOJ which, at its own expense, desires connection through the county MSC. To administer this policy most effectively, a County Control Agency will be designated in each county to coordinate the connection of law enforcement and criminal justice agencies to the CLETS. The Sheriff's Office will serve as the County Control Agency unless DOJ, in consultation with the CAC, indicates another law enforcement agency in the county is better qualified. The single point of entry into each county will be funded by DOJ. Any additional points of entry to the County Control Agency will be at the agency's expense.

The County Control Agency is responsible for providing the CLETS service via its MSC to all qualified CLETS subscribing agencies within their respective county. The cost of the service to subscribing agencies should not reflect more than the actual costs attributed to the MSC's functionality, including any and all hardware, software, interface modules and administrative costs incurred by the County Control Agency.

Any agency desiring to access the CLETS through a County Control Agency must forward the completed application to the County Control Agency which, in turn, will review the application and accompanying system diagram to determine:

1. Eligibility for CLETS service as identified in PPP section 1.3.1.
2. Compliance with PPP section 1.3.2.
3. A need for the CLETS service exists to support the normal activities of the applicant and if facilities such as hardware ports and the physical computer room space are available at the CLETS point of entry into the county or adequate technology is available to serve the applicant. If the room capacity is inadequate or essential facilities are unavailable at the time of application, the County Control Agency will have one budget cycle, approximately 18 months, to accommodate the new subscriber.

Positive findings in these determinations will provide grounds for approval of the application. Negative findings in any of these determinations may be grounds for withholding approval. In either event, the County Control Agency will attach a letter of intent and forward the completed package, along with comments, to DOJ.

B. Upgrade Requirements

When a County Control Agency prepares for an upgrade, the upgrade design must include plans to accommodate all CLETS subscribing agencies with approved access behind their MSC, projected new terminals and any known future CLETS subscribing agencies. It is the responsibility of the County Control Agency to keep the CAS and all affected CLETS subscribing agencies informed in writing of any changes to their MSC by submission of a CLETS upgrade application and MSC/Users Costs and Requirements form (reference Exhibit H).

1.4.5 Direct Interface System Host

A. Roles and Responsibilities

A local agency with a direct interface to the CLETS may provide a CLETS interface to requesting agencies. Agencies wishing to act in the capacity of a Direct Interface System Host do so at their own expense and through an application to DOJ.

The Direct Interface System Host is responsible for providing the CLETS service to CLETS subscribing agencies hosted behind their system. The cost for services provided by the host agency to a subscribing agency will be by agreement between the involved agencies. The determination of whether to host an agency will be at the sole discretion of the Direct Interface System Host.

Any agency desiring to access the CLETS through a Direct Interface System Host must:

1. Provide written notification, no less than 60 days, to the current County Control Agency advising of the plans to change to a Direct Interface System Host, including projected dates, if applicable.
2. Forward a completed application to the Direct Interface System Host agency which, in turn, will review the application and accompanying system diagram for the same criteria as defined for the County Control Agency in PPP section 1.4.4.A.

After review of the application, the Direct Interface System Host will attach a letter of intent and forward the completed package to DOJ. The completed application package should also include a copy of the letter of notification made to the existing host MSC, if applicable.

B. Upgrade Requirements

When a Direct Interface System Host agency prepares for an upgrade, the upgraded design must include plans to accommodate all of the CLETS subscribing agencies with approved access behind the host MSC, projected new terminals and any known future CLETS subscribing agencies. It is the responsibility of the Direct Interface System Host agency to keep the CAS and all affected CLETS subscribing agencies informed in writing of any changes to the host MSC by submission of a CLETS upgrade application and MSC/Users Costs and Requirements form.

C. Termination of Service Requirements

If the Direct Interface System Host wishes to terminate existing service to the subscribing agency, the Direct Interface System Host is responsible for providing CLETS access (under existing terms and conditions of their contract) until another service is available for the subscribing agency, not to exceed six (6) months.

If a subscribing agency wishes to terminate existing service with a Direct Interface System Host, the Direct Interface System Host shall be given sufficient notice and application shall be made for other CLETS access to DOJ.

1.4.6 Local Agency Direct Interface

A. Roles and Responsibilities

Any agency wishing to access the CLETS through a direct interface to DOJ may do so at its own expense and through application to DOJ.

Any agency desiring to access the CLETS through a local agency direct interface must:

1. Provide written notification, no less than 60 days, to the current County Control Agency or Direct Interface System Host, advising of the plans to change to a direct interface and include projected dates, if applicable.
2. Forward a completed application for a direct interface to DOJ. The completed application should include:
 - a. A written justification for the direct interface.
 - b. A written agreement to pay for all circuitry and equipment used to obtain services other than the normal state-provided interface. This is to include any and all hardware, interface modules and administrative costs incurred by DOJ to provide a direct interface capability.
 - c. A copy of the letter of notification made to the current host MSC, if applicable.
 - d. A letter of agreement from the applicant's current CLETS access host, if applicable. The letter of agreement will state the applicant's access to the CLETS will continue through the current host MSC until applicant obtains and initiates direct access.

B. Upgrade Requirements

Once an agency has been approved for a direct interface, it is the agency's responsibility to keep the CAS informed in writing of any changes to the local CLETS interface. Upgrades to a local agency's existing direct interface computer system to the CLETS must be approved through an application to DOJ.

1.4.7 Local Agency Petitioning to Terminate Access through a Direct Interface or a Direct Interface System Host

A. Local Agency Responsibilities

A local agency with a direct interface to the CLETS or an interface through a Direct Interface System Host wishing to terminate such access and return to the resident County Control Agency CLETS connection must send a written request to the County Control Agency.

B. County Control Agency Responsibilities

The County Control Agency must provide a written recommendation to DOJ within 60 days following the local agency's request. The recommendation shall include one of the following:

1. Recommendation for approval for immediate access; or
2. Recommendation for approval for access after a specified time frame.

If the county does not provide a written recommendation within 60 days of the request, recommendation to provide access to the CLETS through the County Control Agency will be considered applicable.

C. Direct Access Appeal

If a local agency petitioning to terminate a direct interface to the CLETS or an interface through a Direct Interface System Host is unable to gain access to the CLETS through the County Control Agency, the matter will be referred to DOJ for review.

1.4.8 Removal of County Control Agency/Direct Interface System Host

In the event it becomes evident to DOJ that an existing County Control Agency/Direct Interface System Host cannot fulfill its responsibilities for any reason, or if a County Control Agency fails to provide CLETS service to qualified applicants or users, it shall be the responsibility of DOJ in consultation with the CAC to seek a remedy through coordination with the County Board of Supervisors or the City Council.

1.5 CONTRACTUAL AGREEMENTS

Any terminal, computer system or other equipment that has access to information from the CLETS, directly or indirectly, must be under the management control of a criminal justice/law enforcement agency authorized by the CLETS Advisory Committee.

Copies of the CLETS-related contractual documents must be retained by the Agency CLETS Coordinator of the CLETS subscribing agency for the duration of the life of the document. Agencies entering into a contractual agreement with a CLETS subscribing agency may be subject to audits and site inspections pursuant to PPP section 1.6.3.

1.5.1 Management Control Agreement

A. Public Agency or Tribe

A Management Control Agreement is required when a public law enforcement, criminal justice agency, or tribal law enforcement agency/court (referred to as the *CLETS subscribing agency*) allows authorized access to CLETS equipment or information from the CLETS to a public or tribal agency that is neither a law enforcement agency nor a criminal justice (CJ) agency (referred to as the *non-CJ agency*).

A signed Management Control Agreement must be received and approved by DOJ prior to the CLETS subscribing agency permitting the non-CJ agency access to CLETS equipment or to information from the CLETS. If a terminal will be placed at a location other than the subscribing agency, an Interagency Agreement (reference Exhibit E) will also be required.

A non-CJ agency may access CLETS equipment or information from the CLETS on behalf of the CLETS subscribing agency to accomplish specified services (such as dispatching, parking citations or data processing/information technology services), if such delegation is authorized pursuant to statute, ordinance, regulation or an agreement between agencies.

The performance of such delegated services by an otherwise non-CJ agency does not convert that agency into a public criminal justice agency, nor does it automatically authorize access to state summary criminal history information or to DOJ/FBI criminal justice databases.

The CLETS subscribing agency will maintain responsibility for security control as it relates to access to the CLETS. Security control is defined as the ability of the CLETS subscribing agency to set, maintain and enforce:

1. Standards for the selection, supervision and termination of personnel. This does not grant hiring/firing authority to the CLETS subscribing agency, only the authority to grant CLETS access to personnel who meet these standards and deny it to those who do not; and
2. Policies governing the operation of computers, access devices, circuits, hubs, boundary protection devices and other components that make up and support a telecommunications network and related DOJ/FBI criminal justice databases used to process, store or transmit criminal justice information, guaranteeing the priority, integrity and availability of service needed by the criminal justice community.

Security controls include, but are not limited to, the supervision of applicable equipment, systems design, programming and operating procedures associated with the development, implementation and operation of any message switching computer or database systems utilized by the served public law enforcement or criminal justice agency or agencies. Computer sites must have adequate physical security to protect against any unauthorized viewing or access to computer terminals, access devices or stored/printed data.

Additionally, it is the responsibility of the CLETS subscribing agency to ensure all non-CJ agency personnel accessing CLETS equipment or information from the CLETS meet the minimum background, training and certification requirements that are also imposed on the CLETS subscribing agency's staff. The minimum requirements are applicable also to staff having access to record storage areas containing information from the CLETS. The minimum requirements of the background security clearance include, but are not limited to:

1. State and FBI fingerprint-based criminal offender record information search. See PPP section 1.9.2 for complete requirements.
2. Each individual must sign a CLETS Employee/Volunteer Statement form prior to operating or having access to CLETS computers, equipment or information. See PPP section 1.9.3.A for complete requirements.
3. All persons having access to the DOJ CLETS-provided information must be trained in the operation, policies and procedures of each file that may be accessed or updated. Training shall be provided only by a certified CLETS/National Crime Information Center (NCIC) trainer and must meet all CLETS training requirements per PPP section 1.8.2.

The CLETS subscribing agency has the responsibility and authority to monitor, audit and enforce the implementation of this agreement by the non-CJ agency.

Information from the CLETS is confidential and shall be used only for the purpose(s) for which it is authorized. Violation of confidentiality requirements or access authorizations may be subject to disciplinary action, civil action and/or criminal charges. Pursuant to PPP section 1.10.1D, if violations occur, the CLETS subscribing agency must include this information on the CLETS Misuse Investigation Reporting Form (reference Exhibit J).

The Management Control Agreement shall be updated when the head of either agency changes or immediately upon request from DOJ.

Exhibit D1 is a sample agreement that meets DOJ and FBI requirements. A management control agreement that is entered into by two or more agencies must incorporate the exact wording of the sample agreement, but may be expanded to meet other requirements of the participating agencies, so long as any expansion is consistent with the language in Exhibit D1.

B. Private Contractor

The Private Contractor Management Control Agreement (reference Exhibit D2) is required when a CLETS subscribing agency allows access to the CLETS equipment or access to record storage areas containing information from the CLETS to a private contractor to perform administration of criminal justice functions such as dispatching or data processing/information services. All requirements established in PPP section 1.5.1.A are applicable for private contractors.

In addition, all private contractors who are given authorized access to the CLETS equipment or information from the CLETS must abide by and sign the FBI CJIS Security Addendum. Vendors with remote access for testing and diagnostic purposes must also enter into a Private Contractor Management Control Agreement specific to their access.

1.5.2 Interagency Agreement for Placement of a CLETS Terminal

Subscribers to the CLETS may place a CLETS terminal with a governmental agency only under the following conditions:

- A. A statute, ordinance or regulation must exist that requires the governmental agency to perform a law enforcement-related function that necessitates receiving information from the CLETS.
- B. The heads of both agencies must sign an "Interagency Agreement," which states all the CLETS/NCIC policies and regulations will be adhered to by all parties involved (reference Exhibit E). The receiving agency will be listed as the secondary location for the terminal.
- C. A copy of the statute, ordinance or regulation and the signed Interagency Agreement must be submitted to DOJ for review and approval prior to the placement of a CLETS terminal.
- D. A terminal mnemonic will be assigned to, and associated with, the CLETS subscribing agency's Originating Agency Identifier, and the CLETS subscribing agency assumes full responsibility and liability for all CLETS activities through the terminal. Pursuant to PPP section 1.10.1D, if violations occur, the CLETS subscribing agency must include this information on the CLETS Misuse Investigation Reporting form (reference Exhibit J).
- E. No terminal will be placed with the governmental agency until all conditions of this agreement are met.
- F. All persons of the governmental agency having access to information from the CLETS are required to undergo a background security clearance to determine their suitability for logical or physical access to CLETS. This includes, at minimum, the required state and federal fingerprint-based criminal offender record information search per PPP section 1.9.2; and each person with access to information from the CLETS must sign the required Employee/Volunteer Statement form (reference Exhibit I).
- G. All persons having access to information from the CLETS must be trained in the operation, policies and procedures of each file that may be accessed or updated. Training can only be provided by the CLETS subscribing agency's certified CLETS/NCIC trainer and must meet all the CLETS/NCIC training requirements per PPP section 1.8.2.

- H. A CLETS subscribing agency may not place a terminal with another agency that meets eligibility requirements for CLETS service. Such an agency must complete an application for new CLETS service.
- I. A copy of the Interagency Agreement must be submitted to DOJ for review, approval or denial and retention in the CLETS subscribing agency's file. The Interagency Agreement shall be updated when the head of the agency changes or immediately upon request from DOJ.

1.5.3 Release of Information from the CLETS

The release of information from the CLETS or the NCIC from a CLETS subscribing agency is bound by the PPP, the FBI CJIS Security Policy (CSP) sections 4.2 and 5.1.1.6 and the California Code of Regulations, title 11, division 1, chapter 7, article 1, section 703 subdivision (b).

If an agency provides information from the CLETS to a non-CLETS subscribing agency, a Release of Information from the CLETS form (reference Exhibit F) must be completed. A copy of this Release of Information from the CLETS form must be submitted to DOJ to review for compliance, approval and retention in the participant's file. The Release of Information from the CLETS form shall be updated when the head of the agency changes or immediately upon request from DOJ. In addition to the completion of the form:

- A. All persons having access to information from the CLETS are required to undergo a background security clearance to determine their suitability for logical or physical access to the CLETS. This includes, at minimum, the required state and federal fingerprint-based criminal offender record information search per PPP section 1.9.2; and must sign the required Employee/Volunteer Statement form (reference Exhibit I).
- B. All persons having access to information from the CLETS must be trained in the operation, policies and procedures of each file that may be accessed or updated. Training shall be provided only by a certified CLETS/NCIC trainer and must meet all the CLETS training requirements per PPP section 1.8.2.
- C. Pursuant to PPP section 1.10.1D, if misuse occurs, the CLETS subscribing agency must include this information on the CLETS Misuse Investigation Reporting form (reference Exhibit J).
- D. All subsequent requests for information by an agency with a current Release of Information from the CLETS form on file will be covered.

1.5.4 Reciprocity Agreement

Any agency that agrees to perform record entry/update and/or hit confirmation functions on behalf of another agency must enter into a Reciprocity Agreement (reference Exhibit G). The Reciprocity Agreement must be signed by the head of each agency and a copy must be submitted to DOJ for approval.

The Reciprocity Agreement shall be updated when the head of the agency changes or immediately upon request from DOJ.

1.5.5 Interstate Access

Pursuant to Government Code section 15162, the CLETS may connect and exchange traffic with compatible systems of adjacent states and otherwise participate in interstate operations. Adjacent state agencies subscribing to the CLETS must adhere to all CLETS policies and regulations.

An Interstate Access Agreement must be completed and submitted to DOJ to review for compliance and retention in the CLETS subscribing agency's file. The Agreement shall be signed by the head of the adjacent state system agency and DOJ.

The Interstate Access Agreement shall be updated when the head of the agency changes or immediately upon request from DOJ.

1.6 SYSTEM RULES

System rules are designed to provide the most efficient operating system consistent with the needs of law enforcement. Adherence to the rules will ensure client agencies the maximum effectiveness of the CLETS. Violations of the PPP or the FBI CJIS Security Policy will result in an investigation and appropriate disciplinary action. Anyone responsible for CLETS misuse is subject to disciplinary action, up to immediate dismissal from employment. Violations of the law may result in criminal and/or civil action.

1.6.1 Database Policies and Regulations

All users shall abide by all policies and regulations pertaining to the information from the CLETS. Procedures and message formats contained in user manuals must be followed exactly.

- A. Users must confirm the validity of the positive response on the record by contacting the entering agency prior to taking enforcement actions based solely on that record.
- B. Periodic driver license checks may be conducted on the CLETS subscribing agency employees where driving is a requirement of their job.
- C. Pursuant to the California Code of Regulations, title 11, division 1, chapter 7, article 1, section 707 subdivision (c), every agency is required to keep a record of each release of criminal offender record information for a minimum of three years from the date of release. Detailed information regarding retention of information can be found in this code section.

Pursuant to California Government Code (GC) section 3, chapter 17.25 (commencing with section 7284,) federal, state or local law enforcement agencies shall not use any non-criminal history information contained within these databases for immigration enforcement purposes. "Immigration enforcement" includes any and all efforts to investigate, enforce, or assist in the investigation or enforcement of any federal civil immigration law, and also includes any and all efforts to investigate, enforce, or assist in the investigation or enforcement of any federal criminal immigration law that penalizes a person's presence in, entry, or reentry to, or employment in, the United States. [GC § 7284.4, subd. (f)]. This restriction does not pertain to

any information that is regarding a person's immigration or citizenship status pursuant to 8 United States Code (U.S.C.) sections 1373 and 1644.

D. DOJ Automated Criminal History System Prohibitions:

1. In reference to U.S.C., title 18, section 922(G)(9), terminals are prohibited from accessing DOJ Automated Criminal History System to enforce the provisions of title 18 U.S.C. section 922(G)(9), which effects a lifetime firearms or ammunition prohibition for anyone convicted of a misdemeanor crime for domestic violence.
2. Terminals are not authorized to access DOJ Automated Criminal History System through the CLETS for licensing, certification or employment purposes, including pre-employment background investigations for sworn peace officers and/or law enforcement employees as specified in Penal Code (PC) section 830, et al; or for remotely accessing a record for review and/or challenge by the subject of a record.

Exceptions:

- a. Pursuant to Education Code section 45125.5 and 35021.1, a law enforcement agency may agree to provide a school district or county office of education specific state summary criminal history information from the CLETS on a prospective non-certificated employee or non-teaching volunteer aide. If the law enforcement agency agrees to provide the state summary criminal history information, the results shall be returned to the requesting district or county office of education within 72 hours of the written request. The law enforcement agency may charge a fee to the requesting agency that must not exceed the actual expense to the law enforcement agency. For purposes of this section only, a school police department may not act as its own law enforcement agency.
- b. Pursuant to PC section 11105.03, a law enforcement agency is authorized to furnish specific state summary criminal history information from the CLETS to a regional, county, city or other local public housing authority for screening prospective participants as well as potential and current staff. The only state summary criminal history information that can be released must be related to adult convictions for specific felonies or a domestic violence offense. Information released to the local public housing authority shall also be released to parole or probation officers at the same time, if applicable. For purposes of this section only, a housing authority police department may not act as its own law enforcement agency unless approved on an individual basis by DOJ.
- c. Pursuant to the Code of Civil Procedure section 1279.5 subdivision (e), the courts shall use the CLETS to determine whether an applicant for a name change is under the jurisdiction of the California Department of Corrections and Rehabilitation or is required to register as a sex offender pursuant to PC section 290. If a court is not equipped with the CLETS, the clerk of the court shall contact an appropriate local law enforcement agency that shall determine whether the applicant is under the jurisdiction of the California Department of Corrections and Rehabilitation or is required to register as a sex offender pursuant to PC section 290.

- d. Pursuant to PC section 11105.6, a law enforcement agency may access state summary criminal history information from the CLETS to notify bail agents if a fugitive has been convicted of a violent felony.
 - e. Pursuant to Welfare and Institutions Code section 16504.5, county child welfare agency personnel conducting an investigation for the purposes described in this code section are entitled to state summary criminal history information from the CLETS by an appropriate governmental agency. Law enforcement personnel shall cooperate with the requests for the information and shall provide the information to the requesting entity in a timely manner.
 - f. Pursuant to California GC section 3, chapter 17.25 (commencing with section 7284,) federal, state or local law enforcement agencies shall not use any non-criminal history information contained within these databases for immigration enforcement purposes. This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to 8 U.S.C. sections 1373 and 1644.
- F. DOJ Automated Criminal History System allowances:
- 1. Staff of any law enforcement or correctional/detention facility may process online criminal offender record information inquiries on any visitor to such facility.
 - 2. A preliminary criminal offender record information search may be performed on any person prior to the approval as a "ride-along" with a law enforcement officer, provided that person is not an employee of the law enforcement agency.
 - 3. In reference to California PC section 13202, access to the DOJ Automated Criminal History System is allowed for law enforcement statistical or research purposes only upon approval by DOJ.

1.6.2 Terminal Mnemonics

A. Static

The term "static" refers to a one-to-one relationship between a mnemonic and a device.

Each CLETS terminal shall have its own unique four-character mnemonic. All the CLETS subscribing sheriffs and police departments must have at least one fixed CLETS terminal with authorization to receive administrative message traffic, unless that agency has an All Points Bulletins Waiver/Release of Liability form on file with DOJ. Message traffic for that terminal must directly terminate at a printer or to a queue of a terminal staffed 24 hours a day/seven days a week. All fixed CLETS terminals receiving hit confirmation requests or locate messages must directly terminate such messages at a printer or to a queue of a terminal staffed 24 hours a day/seven days a week. The CLETS terminal/printer combinations shall have only one mnemonic assigned to the combination, except where a printer may be shared by several terminals.

B. Mnemonic Pooling

Mnemonic pooling is the ability of a mnemonic to represent more than one device and allows a mnemonic to represent a class of users, devices, applications, etc. Mnemonic pooling is only allowed upon approval by DOJ.

A subscribing agency that wants to implement mnemonic pooling must submit an application for mnemonic pooling to DOJ for approval. The form and content of the application will be prescribed by DOJ. All information and requests should be directed to the address listed in PPP section 1.1.3.

1. Mnemonic pooling requires the following:
 - a. The agency must establish an Access Control Point (ACP) to control the dynamic allocation of mnemonics. The ACP shall provide user authentication and auditing of mnemonics.
 - b. The ACPs are required to record all information pertinent to the establishment and maintenance of a connection. Appropriate log entries must be maintained to allow subsequent review of activities that might modify, bypass or negate security safeguards controlled by the computer system, and review of how the ACP handled serious violations.
 - c. The ACPs must log all traffic. The log entries must be maintained for three years to allow subsequent review of all traffic received, whether delivered or not; determine how all traffic was handled; determine when, by date and time, all traffic receipts and deliveries occurred; and determine the individual or the device that received the deliveries.
 - d. Information must be captured and be retrievable from journals maintained by the local switch for three years.
 - e. The ACP will automatically transmit the User ID in the Operator Identification Field (OIF) with the CLETS message (see PPP § 1.6.7) and the terminal address in the Terminal Address Field (TAF), if provided (see PPP § 1.6.8).
 - f. Unsolicited messages cannot be delivered to a pooled mnemonic unless there is a defined destination, such as a printer.

Refer to the *CLETS Technical Guide* for additional technical information about mnemonic pooling.

Each agency must maintain a list of where each terminal is currently located. Such a list shall reside with the designated Agency CLETS Coordinator and must be available for DOJ or FBI inspections. DOJ or FBI staff must be allowed access to any CLETS terminal at any time for audits or other on-site inspections.

Any terminal mnemonic that remains inactive for nine months will be deleted from the CLETS. Inactive mnemonics information will be made available to agencies 90 days prior to deletion.

1.6.3 Audits and Inspections

Periodic unannounced site inspections and scheduled audits may be performed by DOJ or the FBI to ensure compliance with DOJ/FBI policies and regulations. Agencies entering into a contractual agreement with a CLETS subscribing agency may also be subject to these requirements. Authorized personnel performing inspections or audits shall have access to review and/or inspect case files and any records identified in the inspection/audit process, excluding active investigations or cases. The agency being inspected shall produce such records.

1.6.4 Confidentiality of Information from the CLETS

Only authorized law enforcement, criminal justice personnel or their lawfully authorized designees may use a CLETS terminal or have access to information derived from CLETS. Any information from the CLETS is confidential and for official use only. Access is defined as the ability to hear or view any information provided through the CLETS.

It is required that each employee/volunteer/private contractor sign an Employee/Volunteer Statement form (reference Exhibit I) prior to operating or having access to CLETS terminals, equipment or information. This form addresses confidentiality, release and misuse of information from the CLETS.

- A. Information from the CLETS is on a “right-to-know” and “need-to-know” basis.
- B. Authorized personnel shall not inquire into their own record or have someone inquire for them.
- C. Accessing and/or releasing information from the CLETS for non-law enforcement purposes is prohibited, unless otherwise mandated, and is subject to administrative action and/or criminal prosecution.
- D. Pursuant to the PPP section 1.10.1D, all investigations of misuse must be reported to DOJ on the CLETS Misuse Investigation Reporting form (reference Exhibit J), including investigations where misuse was not found.

1.6.5 Administrative Messages

Administrative messages should be as brief and concise as possible while still conveying the desired information. Messages must conform to the examples illustrated in Chapter 2, Administrative Messages, and in Chapter 7, All Points Bulletins, of the *CLETS Operating Manual*.

1.6.6 Local/Wide Area Networks – Definition and Requirements

A Local Area Network (LAN) or a Wide Area Network (WAN) is that portion of the hardware and software that is designed to pass intra-LAN, city/county data and CLETS messages directly to the CLETS or through the local message switching computer (MSC). For CLETS purposes, a system with LAN characteristics will be considered a LAN. With myriad LAN/WAN products available to law enforcement today, the following specifications are required for those systems connected to the CLETS:

- A. A LAN/WAN system upgrade application and diagram shall be submitted to DOJ. The application package shall include standards, protocols, operating systems, servers, the type of security and how it is being used.
- B. Each LAN/WAN workstation and/or communication server shall have an auditable address assigned as a CLETS mnemonic. No random selection or pooling of the CLETS mnemonics is allowed unless a mnemonic pooling alternative has been approved for implementation.
- C. All CLETS messages transmitted through a host system may contain an optional supplemental header of up to 40 characters. Please refer to the CLETS Technical Guide available on CLEW for more information.
 - 1. LANs using Transmission Control Protocol/Internet Protocol (TCP/IP) can transmit the Internet Protocol (IP) and Media Access Control (MAC) addresses, if available, in the TAF as referenced in PPP section 1.6.8.B.
 - 2. All LAN-based terminals, regardless of the type of protocol used, should transmit an address equivalent to the MAC. If an IP address is not used or is not available, the MAC address should appear in the first six characters of the TAF. If neither is available, some other uniquely identifying information should be provided.
- D. Non-law enforcement and non-criminal justice agency terminals connected to the LAN/WAN must be prohibited from accessing information from the CLETS unless authorized by contractual agreements as specified in PPP section 1.5.

1.6.7 Operator Identification Field (OIF) Requirements

All MSC, Computer Aided Dispatch (CAD) systems and LAN/WAN systems must transmit a unique User ID. The OIF shall be comprised of three to 32 characters and terminated by a period. Please refer to the CLETS Technical Guide available on CLEW for more information.

- A. Each person authorized to store, process and/or transmit information from the CLETS shall be uniquely identified with a User ID and password. The User ID can take the form of a name, badge number, serial number or other unique number.
- B. Each terminal operator must log on with his or her unique User ID and password and is accountable for all transactions transmitted under that User ID and password. The User ID must be stored by the local MSC/CAD/LAN/WAN or other host server, be available for retrieval and be consistent with journal requirements. User IDs are to be unique to each individual and not reassigned unless there is at least a six-month period between each use. Using another operator's unique User ID and password is a violation.
- C. The local host server will automatically transmit only the User ID with each message transaction to the CLETS in the OIF.
- D. The CLETS will accept the OIF information and store the data in the CLETS journal records.

1.6.8 Terminal Address Field (TAF) Requirements

All MSC, CAD and LAN/WAN systems may transmit an optional TAF. The TAF is a six- to 18-character variable length field following and separated from the OIF by a period, identified by a number sign and terminated by a period. Please refer to the CLETS Technical Guide available on CLEW for more information.

- A. How the TAF is used depends on the method of identification the agency wishes to use.
- B. LANs using TCP/IP can transmit the IP and MAC addresses in the TAF.
- C. If neither an IP nor a MAC address is available, the information used by the agency to uniquely identify the terminal should be entered.

1.7 SYSTEM DESIGN AND ENHANCEMENT STANDARDS

1.7.1 Message Switching Computer (MSC) Definition and Requirements

An MSC is that portion of the hardware and software solely designed to pass transactions to and from the CLETS. The MSCs shall be maintained with a 98% availability and uptime measured over a continuous 12-month period, including all (scheduled and unscheduled) downtime.

- A. All direct interface MSCs shall record all transactions to and from the CLETS, in their entirety, on an automated log or journal and shall have the capability to search and print all journals for a three-year period. The journals shall identify the User ID log-on and the authorizing agency on all transactions. Access to the journals must be highly controlled. Criminal history transactions on the journals that also identify the requester and secondary recipient shall meet criminal offender record information audit requirements. A secondary optional field located after the text should be used to identify a requester other than the CLETS terminal operator.
- B. All MSCs interfaced with the CLETS must follow the requirements adopted by DOJ and the FBI CJIS Security Policy covering such interfaces.

1.7.2 MSC Design

All MSCs planning to upgrade or relocate must formally advise DOJ at least 90 days in advance of the move with the new address, planned move/implementation date and whether test lines and terminal mnemonics are required.

1.7.3 System Upgrade

An upgrade consists of any installation, replacement or planned enhancement of software or hardware that has a direct impact on the CLETS by a directly or indirectly connected host server of a CLETS subscribing agency.

- A. The subscribing agency shall forward a completed upgrade application to the County Control Agency/Direct Interface System Host for review and recommendation (see PPP §§ 1.4.3 and 1.4.4). The County Control Agency/Direct Interface System Host shall send the application along with comments to DOJ.
- B. An electronic one-page, no-longer-than-legal-size, color network configuration diagram is required with all upgrade applications and must include the subscribing agency's entire network that accesses the CLETS and all other networks and users connected to the network.

The diagram shall identify the following, if applicable:

- Agency name, county, and date;
- Agency ORI;
- Diagram must indicate "CONFIDENTIAL;"
- The path of all CLETS traffic, both fixed and mobile, from the subscribing agency to DOJ;

- All systems (e.g., RMS, CAD, MSC, etc.);
- Each individual network (e.g., City, County, etc.);
- Physically secured locations (indicate encryption, boundary protection devices, such as firewalls, and identify the controlling agency who manages the device);
- CLETS access and/or hardware located in different buildings including the addresses and encryption/boundary protection between the network segments;
- Public network segments used to transport CLETS traffic;
- Internet access that exists within the network (indicate boundary protection devices and who manages the device);
- Wireless access (e.g., satellite, microwave, Wi-Fi, cellular, etc.);
- All points of encryption and decryption including algorithms (e.g., AES) & levels (e.g., 128-bit, 256-bit);
- Remote access and by whom it will be accessed (e.g., employee, vendor, etc.); and
- Multi-factor authentication.

C. An upgrade application submitted by a County Control Agency must include an MSC/Users Costs and Requirements form (reference Exhibit H). The County Control Agency must certify that each of the CLETS subscribing agencies behind their interface is informed of all costs and/or requirements, if any, associated with the upgraded system (e.g., costs using a specified formula and listing cost ranges, specific equipment, county database access and cost, etc.). This information should be advanced to all affected agencies approximately 18 months prior to production for budgeting and planning purposes.

1.7.4 MSC Test Lines

An agency upgrading its system may need to conduct testing prior to production implementation. Once an upgrade application has been approved by DOJ, the agency must request a test line and any test mnemonics in writing from DOJ. During the testing period of a new or upgraded system, the agency is responsible for the line, equipment (modems, line drivers, etc.) and installation costs. Testing of upgraded equipment shall not exceed one year unless by written consent of DOJ.

DOJ will assume line and equipment costs when the system begins production for County Control Agencies only and at such time as the previous, DOJ-provided interface is disconnected. Upon production, the County Control Agency is responsible for sending a letter to DOJ requesting the test line and test mnemonics be deleted and that charges be transferred to DOJ. Copies of the latest bills shall be included with this request.

1.8 TRAINING

1.8.1 System Training

Agencies with host systems are responsible for training their local users on how to access the message switching computer (MSC) and the use of pre-formatted screens.

1.8.2 Database Training

Training in message formats for access to information in DOJ criminal justice databases, the National Crime Information Center (NCIC), the International Justice and Public Safety Network (Nlets), and the Department of Motor Vehicles is the responsibility of DOJ. Training will be accomplished according to the following:

- A. All city, county, state and federal agencies that use information from the CLETS must participate in DOJ's training programs to ensure all personnel are trained in the operation, policies and regulations of each file that is accessed or updated. Training must include the requirement that CLETS information shall only be obtained in the course of official business. The person receiving this information must have a "right to know" and "need to know"; and must have been trained in the possible sanctions and/or criminal/civil liabilities if the information is misused. Training shall be provided only by DOJ's training staff or another certified CLETS/NCIC trainer.

Specifically, the training requirements are as follows:

1. Initially (prior to accessing Criminal Justice Information [CJI]), train, functionally test and affirm the proficiency of all terminal (equipment) operators (full access/less than full access) to ensure compliance with the CLETS/NCIC policies and regulations. This is accomplished by completing the required training and the appropriate CLETS/NCIC Telecommunications Proficiency Examination published by DOJ, or a facsimile thereof. An agency wishing to make additions or modifications to the Proficiency Examination must receive prior approval from DOJ.
2. Annually provide functional retesting and reaffirm the proficiency of all terminal (equipment) operators (full access/less than full access) to ensure compliance with the CLETS/NCIC policies and regulations. This is accomplished by the completion of the appropriate CLETS/NCIC Telecommunications Proficiency Examination published by DOJ, or a facsimile thereof. An agency wishing to make additions or modifications to the Proficiency Examination must receive prior approval from DOJ.
3. Maintain records of all training, testing and proficiency affirmation. Training records, written or electronic, shall identify the individual's CLETS category of Full Access operator, Less Than Full Access operator, Practitioner or Administrator. The records must record the date of initial CLETS training and, for operators, the date(s) the initial and subsequent annual Telecommunications Proficiency Examination were completed, recording a passing score of 70% or better or a pass/fail notation. The examinations may be discarded or returned to the operator upon entry of the required information in the appropriate log. Retain individual training records for a minimum of three years.
4. Initially (prior to accessing CJI), all sworn/non-sworn practitioner personnel must receive basic training in the CLETS/NCIC policies, liability issues and regulations. Practitioner is defined as any person who has ongoing access to information from the CLETS and is not a CLETS operator.
5. Make available appropriate training on the CLETS/NCIC system for criminal justice practitioners other than sworn personnel.

6. All sworn law enforcement personnel and other practitioners should be provided with continuing access to information concerning the CLETS/NCIC systems, using methods such as roll call and in-service training.
 7. Provide peer-level training on the CLETS/NCIC system use, regulations, policies, audits, sanctions and related civil liability for criminal justice administrators and upper-level managers. Training is accomplished by reviewing and signing for the NCIC “Areas of Liability for the Criminal Justice Information System Administrator” packet.
- B. To ensure compliance with this training mandate, DOJ is responsible for monitoring the ongoing training provided to law enforcement personnel. On-site visits, including classroom observation and review of training records, may be conducted by DOJ staff.

1.8.3 Security Awareness Training

Security and awareness training shall be required for all personnel who have direct or indirect access to CLETS systems and shall meet the requirements specified in the FBI CJIS Security Policy section 5.2.

1.9 OPERATIONAL CONTROL, OVERSIGHT and COMPLIANCE RESPONSIBILITY

Statewide operational control and system supervision shall be under the direction of DOJ. Monitoring of traffic for conformity to policies, regulations and recommendations for corrective actions shall also be the responsibility of DOJ. The responsibility for maintaining the security and confidentiality of criminal justice information rests with the individual agency head.

Agencies with systems interfacing with or to the CLETS shall assist DOJ in overseeing new and upgrades of application hardware, software and security of the terminals connected to the computer system for compliance with the PPP and FBI CJIS Security Policy (CSP). At the discretion of the agency head, vendors may remotely access the CLETS for testing and diagnostic purposes only after execution of a CLETS Private Contractor Management Control Agreement (reference Exhibit D2).

1.9.1 Information Technology (IT) Security Incident Response Reporting

Agencies shall immediately notify DOJ of security incidents or data breaches. Such incidents shall be reported to the 24/7 DOJ Computer Operations Team at 916-210-3500. This information shall also be reported by email to the CLETS Administration Section at CAS@doj.ca.gov via the CLETS IT Security Incident Response Form (reference Exhibit L). Security incidents identified as system misuse shall be reported on the annual CLETS Misuse Investigation Reporting form (reference Exhibit J). The Incident Response Plan for your agency must include these notification requirements.

1.9.2 Background and Fingerprint-Based Criminal Offender Record Information Search

A. All persons, including non-criminal justice, volunteer personnel, private vendor technical or maintenance personnel with physical or logical access to the CLETS equipment, information from the CLETS or to criminal offender record information, are required to undergo a background security clearance to determine their suitability for logical or physical access to CLETS. This includes, at a minimum, a state and federal fingerprint-based criminal offender record information search pursuant to the California Code of Regulations, title 11, division 1, chapter 7, article 1, sections 703 subdivision (d) and 707 subdivision (b). Unescorted access to a law enforcement or criminal justice agency's secure environment requires submission of a state and federal fingerprint-based background security check to DOJ using the law enforcement agency Originating Agency Identifier (ORI). All other fingerprint-based employment background checks are not valid for access to CLETS (i.e., if applicable personnel are fingerprinted under a non-law enforcement agency ORI for hiring purposes, they must also undergo a state and federal fingerprint-based background security check under a law enforcement ORI to determine their suitability for logical or physical access to CLETS).

1. Pursuant to the FBI CSP § section 5.12, if the state and federal fingerprint-based criminal offender record information search reveals a felony conviction of any kind, CLETS/NCIC access shall not be granted. If it is revealed the person appears to be a fugitive or has an arrest history without conviction for a felony, the agency head or his/her designee will review the matter and decide if CLETS access is appropriate.

2. Visitors to a computer center (e.g., tour group, delivery, janitorial or maintenance personnel) where the computer center has criminal offender record information access are not required to undergo a state and federal fingerprint-based criminal offender record information search. They must, however, be escorted at all times.
 3. The final responsibility for maintaining the security and confidentiality of criminal justice information rests with the individual agency head.
- B. Personnel authorized terminal access to the CLETS may be sworn law enforcement or criminal justice personnel, non-sworn law enforcement or criminal justice personnel, volunteer personnel and private vendor technical or maintenance personnel who have been subjected to a background security clearance to include, at a minimum, the following checks:
1. A DOJ fingerprint-based criminal offender record information search.
 2. An FBI fingerprint-based criminal offender record information search.
 3. Additionally, DOJ criminal justice databases may be accessed for background investigation of law enforcement and criminal justice employees, with the exception of the Automated Criminal History and Mental Health Firearms Prohibition Systems.
- C. Personnel shall not operate or have access to CLETS terminals, equipment or information until, at a minimum, a state and federal fingerprint-based criminal offender record information search is completed and approved by the agency head. Following approval of the completed investigation, a memorandum or other notation should be retained either in the employee's personnel file or in another pertinent file indicating authorization has been granted.

Suitability for CLETS access following, at a minimum, the completed state and federal fingerprint-based check criminal offender record information search is at the discretion of the agency head. In all matters pertaining to personnel security, the agency head will be responsible for making the final determination of the individual's suitability for the job.

1.9.3 User Access

- A. It is required that each employee/volunteer sign an Employee/Volunteer Statement form (reference Exhibit I) prior to operating or having access to the CLETS terminals, equipment or information. It is recommended that each employee/volunteer sign an Employee/Volunteer Statement form on a biennial basis. Additional requirements may be added at an agency's discretion. Any addition cannot negate the intent of the Employee/Volunteer Statement form.
- B. The agency shall validate system accounts including establishing, activating, modifying, reviewing, disabling and removing accounts, at least annually, and shall document the validation process.
- C. When a person with access to the CLETS is no longer employed or no longer accessing the CLETS on behalf of law enforcement or a criminal justice agency, the agency is

responsible for immediately removing all related passwords, security authorizations, tokens, etc., from the system.

1.9.4 Non-Federal, Non-State, and Non-Local Governmental Employees

All persons who are not federal, state, or local governmental employees, who are exercising law enforcement powers as part of a Criminal Justice and/or Law Enforcement Agency, as defined in the PPP Glossary, shall meet all of the California Peace Officer Standards and Training mandated requirements to be a California peace officer, in addition to those requirements set forth in PPP sections 1.9.2 and 1.9.3. Such law enforcement officers shall also be deputized by a federal, state or local law enforcement agency and provide copies of the relevant deputization agreements at the time of application for CLETS access to DOJ systems.

Tribal law enforcement agencies shall submit applicable law enforcement certifications and/or deputization agreements at the time of application for CLETS access to DOJ systems.

1.9.5 System Use Notification Recommendation

In addition to the requirements identified in FBI CSP section 5.5.4, it is recommended that agencies include the statement below regarding the California Values Act (Senate Bill 54) to their system use notification and governance policies:

“Federal, state or local law enforcement agencies shall not use any non-criminal history information contained within these databases for immigration enforcement purposes. This restriction does not pertain to any information that is regarding a person’s immigration or citizenship status pursuant to 8 U.S.C. § 1373 and § 1644.”

These recommended guidelines will ensure information is limited for immigration enforcement purposes, to the fullest extent practicable, and consistent with federal and state law.

1.10 SYSTEM DISCIPLINE/APPEAL PROCESS

Pursuant to Government Code section 15154, DOJ is responsible for overseeing system discipline with the assistance of the CLETS Advisory Committee (CAC). System misuse is taken very seriously and anyone responsible for CLETS misuse is subject to disciplinary action, up to immediate dismissal from employment. Violations of the law may result in criminal and/or civil action. Messages/transactions processed through the CLETS shall be subject to random sampling by DOJ, or its designee(s), for validity of content and conformity with CLETS policies and regulations.

1.10.1 System Misuse

- A. Violations of the PPP shall be investigated by the agency head or his/her designee and reported to DOJ.

Misuse is defined as the CLETS information obtained or provided outside the course of official business; a "right to know" and the "need to know" must be established. The "right to know" is defined as "authorized access to such records by statute" and the "need to know" is defined as "the information is required for the performance of official duties or functions." Other than blatant misuse, the following are examples of prohibited/unauthorized use of the CLETS by federal, state or local law enforcement agencies that include, but are not limited to:

- Querying yourself, family members, romantic partners, business associates, friends, neighbors, etc;
- Providing information from the CLETS to another officer, individual, agency or company for unauthorized purposes;
- Sharing user IDs or passwords;
- Logging into the CLETS and allowing others to utilize your authorized access;
- Querying the Automated Criminal History System for licensing, employment or certification purposes (e.g., Carry Concealed Weapon permits);
- Querying a firearm to determine if it is stolen prior to purchase;
- Querying the Department of Motor Vehicles to obtain unauthorized address, vehicle registration, or insurance information (e.g., querying a vehicle parked in front of your house for two days);
- Querying individuals from high profile cases covered by the media for inquisitorial purposes; and
- Using any non-criminal history information contained within these databases for immigration enforcement purposes. This restriction does not pertain to information that is regarding a person's immigration or citizenship status pursuant to 8 United States Code sections 1373 and 1644.

The agency head or his/her designee shall investigate incidents of system misuse by reviewing its internal processes, documentation and the PPP for authorized usage. In the event the agency head requires assistance from DOJ in conducting a journal search of the CLETS transactions, a written request on agency letterhead, signed by a supervisor or agency head, shall be submitted to DOJ. Any information as a result of the journal search will be provided to the agency head in writing. The agency head shall return an assessment of the investigation and statement of corrective action to DOJ.

If the reported explanation and corrective actions resolve the problem, the investigation and results will be reported to the CAC by DOJ.

If the reported explanation and corrective actions do not resolve the problem to the satisfaction of DOJ, the head of the agency may be requested to appear before the CAC to explain the incident.

Unresolved incidents shall be presented to the CAC by the CLETS Executive Secretary. The CAC will recommend a course of action or sanction to apply. DOJ will issue a letter formally notifying the agency of the decision.

- B. In the event of a violation of law or if the PPP results in system misuse, DOJ, with a recommendation from the CAC, will take appropriate action such as:
 - 1. Letter of censure;
 - 2. Suspension of service for an individual or agency. This may be for varying lengths of time and/or may include suspension for a specified database or other system services; and/or
 - 3. Removal of the CLETS service for an individual or agency. Please note: two or more instances of misuse may result in removal of CLETS access for an individual.
- C. In the event the agency is scheduled to report to the CAC under the provisions of PPP section 1.10.1.A, the agency head shall have a minimum of two weeks' notice prior to the meeting. All pertinent information shall be made available to the agency head to assist the agency in preparing to address the issue.

If a sanction is recommended by the CAC, the effective date of the action shall be 10 working days. The 10-day notice can be waived if extraordinary circumstances exist.

If the agency head chooses to appeal the action, the request for review or reconsideration shall be forwarded to the Attorney General within 10 working days from the date of the action. If no such request is received within that time frame, the action shall be considered final.
- D. All CLETS subscribing agencies shall submit a report to DOJ of investigations performed related to CLETS misuse and any disciplinary action taken. This report shall be submitted by February 1st of each year, for the prior calendar, even if no misuse occurred. This information will be submitted on the CLETS Misuse Investigation Reporting form (reference Exhibit J) and must detail the number of misuse investigations performed, the type of misuse and the outcome.
 - a. Agencies that reported misuse as pending must notify DOJ of the outcome and any disciplinary action taken, immediately upon resolution.
 - b. Failure to submit the required form will result in the agency name being posted on the Attorney General's website and the CLEW; and additional sanctions as described in PPP section 1.10.1B may apply.

1.10.2 Discontinuance of CLETS Service

DOJ or the subscriber may, upon 30 days' written notice, discontinue service.

FBI CJIS Security Policy (CSP)

Area Reference

The PPP defers to the FBI CSP for the technical security requirements. The following is provided as a reference to the policy areas that are contained within the FBI CSP section 5.

Policy Area 1	Information Exchange Agreements
Policy Area 2	Security Awareness Training
Policy Area 3	Incident Response
Policy Area 4	Auditing and Accountability
Policy Area 5	Access Control
Policy Area 6	Identification and Authentication
Policy Area 7	Configuration Management
Policy Area 8	Media Protection
Policy Area 9	Physical Protection
Policy Area 10	System and Communications Protection and Information Integrity
Policy Area 11	Formal Audits
Policy Area 12	Personnel Security
Policy Area 13	Mobile Devices

The Appendix includes information exchange agreements and the FBI CJIS Security Addendum.

GLOSSARY

Access Control Point: The first point at which the integrity and security of a California Law Enforcement Telecommunications System (CLETS) connection is authenticated and audited, whether it is a direct Message Switching Computer (MSC), an indirect MSC or an indirect MSC several layers removed from the Direct MSC.

Administrative Message: A point-to-point CLETS message (including All Points Bulletins) sent from a terminal and destined for one or more terminals.

Agency CLETS Coordinator (ACC): The individual designated to be an agency's certified CLETS user trainer and terminal coordinator; acts as liaison between the agency and the DOJ CLETS Administration Section (CAS) in all CLETS functions.

All Points Bulletin: An administrative message sent from a terminal and destined for a group code to distribute the message to multiple terminals throughout the county, state or nation.

Application: Formal qualifying paperwork to be filed with DOJ through the CLETS Executive Secretary when new or upgraded service is requested.

Automated Boat System (ABS): The DOJ criminal justice database containing information regarding stolen, recovered, stored, repossessed and embezzled vessels.

Automated Criminal History System (ACHS): The DOJ criminal justice database containing compiled records of arrest and court disposition information on subjects.

Automated Firearms System (AFS): The DOJ criminal justice database containing information regarding firearms registration and lost, stolen or seized firearms.

Automated Property System (APS): The DOJ criminal justice database containing information regarding lost or stolen property.

Boundary Protection Device: Monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. Examples of boundary protection devices are proxies, gateways, guards, routers, firewalls and encryption tunnels.

DOJ Criminal Justice Databases: The computerized California data files at DOJ and maintained by local law enforcement agencies and/or DOJ. Data files include: the Automated Firearms System (AFS), the Automated Property System (APS), the Automated Criminal History System (ACHS), the California Restraining and Protective Order System (CARPOS), the Mental Health Firearms Prohibition System (MHFPS), the Missing/Unidentified Persons System (MUPS), the Supervised Release File (SRF), the Stolen Vehicle System (SVS)/Automated Boat System (ABS), the Wanted Persons System (WPS), and the California Sex and Arson Registration System (CSAR).

California Department of Justice (DOJ): The California state department that maintains and operates the CLETS and the criminal justice databases; acts as the National Criminal Information Center (NCIC) and the International Justice and Public Safety Network (Nlets) control terminal agency for California and performs numerous service functions for law enforcement agencies;

responsible for investigating allegations of CLETS misuse; develops all technical requirements for access to CLETS by computer systems.

California Law Enforcement Telecommunications System (CLETS): The computerized telecommunications system in the State of California that is used by public agencies of law enforcement and criminal justice for accessing law enforcement information and sending law enforcement messages.

California Restraining and Protective Order System (CARPOS): The DOJ criminal justice database containing information regarding active restraining orders in addition to containing historical data on restraining orders that have expired within the past five years. The CARPOS also allows law enforcement to send a Violation Message to the CARPOS containing information on a possible violation of the restraining order.

California Sex and Arson Registry (CSAR): The DOJ criminal justice database containing information regarding sex and arson registrants. The information available in CSAR includes risk assessment information, method of operation information, employment and vehicle information, sexually violent predator status and registrant photos.

CLETS Administration Section (CAS): The DOJ unit that administratively manages the CLETS network; issues terminal mnemonics and their access authorizations; provides technical consultation services to the CLETS clients for planning and implementing new and upgrading MSC systems; provides staff support to the CLETS Advisory Committee.

CLETS Advisory Committee (CAC): The 10-member committee governed under California Government Code section 15154 to advise and assist the Attorney General in the management of the CLETS with respect to operating policies, service evaluation and system discipline.

CLETS Executive Secretary: Provides staff support to the CAC and is manager of the CAS; facilitates investigations of alleged CLETS misuse; develops and enforces all CAC-approved policies and CLETS security requirements; facilitates in the development of technical requirements for access to CLETS by computer systems; and oversees the assignment of all CLETS terminal mnemonics and access authorizations.

Computer Aided Dispatch (CAD): A computerized system used by law enforcement agencies for dispatching and message switching services.

County Control Agency: The designated agency in each county that is provided the circuits by DOJ to serve approved CLETS subscribers within that county.

Criminal Justice Agency: A public agency whose primary purpose is detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, rehabilitation of accused persons or criminal offenders, criminal identification activities, and the collection, storage and dissemination of criminal history record information. Agencies include district attorneys, courts, probation/parole departments, correctional facilities or offices.

Criminal Offender Record Information (CORI): Criminal history arrest information regarding a subject or subjects retained by/at any governmental entity therein is considered CORI, and falls under the CORI rules and regulations.

Department of Motor Vehicles (DMV): The California department that maintains the state's data files containing driver license, automated name index and vehicle registration information.

Dial-Up Access: A method of transporting the CLETS messages using public switched telephone lines that are available through special application only.

Direct Access: Accessing the CLETS with a direct line to DOJ rather than via the county control agency's MSC.

Direct Interface System Host: A non-county control agency with a direct interface to the CLETS, which provides host message switching services to the CLETS for other agencies.

FBI Criminal Justice Information Services (CJIS) Security Policy (CSP): The minimum level of Information Technology security **requirements** determined by the FBI as acceptable for the transmission, processing and storage of national and state criminal justice data.

Interagency Agreement: An agreement between a CLETS Subscribing Agency and a governmental agency. This agreement allows the CLETS Subscribing Agency to provide a CLETS terminal with the governmental agency that is entitled to receive the information through statute, regulation or ordinance under conditional agreements.

Interstate Identification Index (III): III is the decentralization of the FBI/NCIC criminal history subject files. When a query of III is received, NCIC responds with the full criminal record information from non-III participating states, and identifies the III-participating states maintaining criminal history files on the subject. NCIC then automatically forwards the query to the III-participating states with records on the subject, and the individual states must respond back to the original inquirer with the criminal history information from their state. III promotes the interstate exchange of criminal history information, with each III participant maintaining its own state's criminal history records, rather than the NCIC.

Journal Record: A computer-generated record of the CLETS message(s). DOJ requires every CLETS MSC to completely record all CLETS transactions, incoming and outgoing, and to be able to retrieve them using search parameters for at least three years. DOJ retains all the CLETS transactions for three years with statewide journal search capabilities. In addition, the DOJ ACHS journals all criminal history queries with no time limit on searches.

Law Enforcement Agency: A public agency having statutory power of arrest and whose primary function is that of apprehension and detection. Agencies include sheriffs, city police departments, the California Highway Patrol, DOJ and the FBI.

Local Area Network (LAN): A network of personal computers administered by a single host server through a "sharing environment". LANs may interface with the CLETS either directly or indirectly if all application and security requirements are met.

Management Control Agreement (MCA): There are two MCAs: one for use with a public agency, the other for use with a private contractor. The MCA is a CLETS agreement required when a CLETS subscriber agency does not maintain physical and/or operational control of its terminals or equipment hardware and software. The agreement states that the law enforcement agency maintains management control to set policy, priorities and assignment of personnel associated with the CLETS-connected equipment and must be signed by the heads of both agencies.

Media Access Control (MAC) Address: The hardwired port address of a Local Area Network (LAN)-based terminal.

Mental Health Firearms Prohibition System (MHFPS): The DOJ criminal justice database containing information regarding individuals who are prohibited from owning or carrying a firearm due to mental health restraints.

Message Switching Computer (MSC): The portion of the hardware and software solely designed to switch transactions to and from the CLETS.

Missing/Unidentified Persons System (MUPS): The DOJ criminal justice databases containing information regarding missing persons and unidentified living or deceased persons.

Mnemonic Pooling: The ability for a mnemonic to represent more than one device, which allows a mnemonic to represent a class of users, devices, applications, etc.

Mobile Data Terminal (MDT): A CLETS terminal with mobile capability, usually located in a patrol car, and which includes laptops, handheld devices or other transportables.

MSC Administrator: The individual responsible for coordinating CLETS-related issues with DOJ.

National Crime Information Center (NCIC): The nationwide computerized data files maintained by the Federal Bureau of Investigation (FBI), and composed of data files similar to those in the DOJ criminal justice databases, but at the national level. The NCIC files include additional files not duplicated by DOJ.

National Law Enforcement Telecommunications System (Nlets): The interstate computerized telecommunications backbone system that provides a connection to every state, allowing law enforcement agencies to send/receive information from other states' databases and law enforcement agencies.

Need-to-know: The necessity to obtain DOJ or FBI information to execute official responsibilities.

Operator Identification Field (OIF): A field containing three to 32 alpha/numeric characters that identify the terminal operator's User ID. The OIF is required for all terminals and users accessing the CLETS from behind a computer system.

Originating Agency Identifier (ORI): The nine-character alpha/numeric "number" issued by the FBI/NCIC that identifies and entitles a law enforcement or criminal justice agency to receive law enforcement information.

Right-to-know: The right to obtain DOJ or FBI information pursuant to court order, statute or decisional law.

Static Terminal Mnemonic: (see Terminal Mnemonic, Static)

Stolen Vehicle System (SVS): The DOJ criminal justice database containing information regarding lost, stolen, stored or impounded vehicles, vehicle license plates or vehicle parts.

Subscriber Agreement: A required agreement for participation in the CLETS signed by the head of each subscriber agency. The agreement states the subscriber will abide by all rules, requirements, policies, practices and procedures established by the CLETS, the NCIC, the Nlets and the DOJ criminal justice databases.

Sub-Unit of a Public Agency: A unit of a non-law enforcement public agency that performs the duties of a law enforcement agency, whose employees are peace officers, and the majority of whose annual budget (more than 50%) is allocated to the administration of criminal justice. Sub-units include local, state or federal agencies such as the Department of Insurance-Fraud Division; the Employment Development Department-Investigations Bureau; the military police; and the fire department-arson investigations units.

Supervised Release File (SRF): A DOJ criminal justice database of active California Department of Corrections and Rehabilitation and California Youth Authority parolees, county and federal probationers, sex and arson registrants, violent offenders and career criminals. The SRF allows law enforcement to send a Contact Message advising the supervising officer of all encounters with the subject.

Supplemental Header: An optional field that may contain up to 40 characters containing alpha/numeric characters generated from a message switching computer with every CLETS transaction and returned with every response.

Transmission Control Protocol/Internet Protocol (TCP/IP): A type of message transmission method used by LAN-based terminals and used by DOJ as the primary means of line connection to a direct interface message switching computer.

Terminal: The access device used to access CLETS, including both fixed and mobile devices. The terminals include but are not limited to: desktop workstations, mobile data computers (MDC), laptops, and handheld devices.

Terminal Address Field: An optional field that may contain six to 18 alpha/numeric characters that include a terminal's Internet Protocol (IP) and/or MAC addresses.

Terminal Mnemonic: The four-character address (terminal name) assigned by DOJ's CAS to identify each CLETS terminal. The terminal mnemonic is transmitted with each CLETS message in the first four characters of the supplemental header.

Terminal Mnemonic, Static: A term reflecting the one-to-one relationship between a mnemonic and a device.

Time Activated Message Forwarding (TAMF): The CLETS programming feature that allows a specific terminal's messages to be automatically forwarded to another designated terminal on a temporary or continuous basis on specific days and times, e.g., daily from 5 p.m. to 7 a.m.

Tribe: A federally recognized Indian Tribe whose territorial boundaries lie wholly or partially within the State of California, and any agencies, entities, or arms of the tribe, as applicable, either together or separately.

User ID: Information determining the identity of a terminal operator and transmitted in the six-character OIF with each CLETS transaction.

Volunteer Personnel: Agency personnel who may include individuals, such as Reserves, law enforcement Explorer Scouts, law enforcement cadets, student workers and senior citizen volunteers.

Wanted Persons System (WPS): The DOJ criminal justice database containing information regarding persons with outstanding arrest warrants in California.

Wide Area Network (WAN): A network of multiple LAN hosted by a common server. LAN/WANs may interface with the CLETS either directly or indirectly if all application and security requirements are met.