

CLETS POLICIES, PRACTICES and PROCEDURES

Table of Contents

<u>SECTION</u>	<u>SUBJECT</u>	<u>PAGE</u>
	<u>SUMMARY</u>	v
1.0	<u>LEGISLATIVE INTENT AND LAW</u>	1
	1.0.1 California Government Code – Chapter 2.5	
1.1	<u>PURPOSE AND SYSTEM DESCRIPTION</u>	5
	1.1.1 Purpose of the CLETS	
	1.1.2 State Provided Services	
	1.1.3 Request for General Information	
1.2	<u>THE CLETS ADVISORY COMMITTEE</u>	6
	1.2.1 Responsibilities of Committee	
	1.2.2 Subcommittees	
	1.2.3 Committee Member Consultation	
	1.2.4 The CAC Meetings	
1.3	<u>QUALIFICATIONS FOR MEMBERSHIP IN THE CLETS</u>	7
	1.3.1 Eligibility for the CLETS Service	
	1.3.2 Applicant Request for Service	
	1.3.3 Subscriber Agreement	
	1.3.4 Agency CLETS Coordinator	
	1.3.5 Security Points of Contact	
1.4	<u>THE CLETS INTERFACES</u>	910
	1.4.1 Connections	
	1.4.2 Requirements for Both County Control Agency and Direct Interface System Host	
	1.4.3 County Control Agency	
	1.4.4 Direct Interface System Host	

<u>SECTION</u>	<u>SUBJECT</u>	<u>PAGE</u>
	1.4.5 Local Agency Direct Interface	
	1.4.6 Local Agency Petitioning to Terminate Access through a Direct Interface or a Direct Interface System Host	
	1.4.7 Removal of County Control Agency/Direct Interface System Host	
1.5	<u>CONTRACTUAL AGREEMENTS</u>	1718
	1.5.1 Management Control Agreement	
	1.5.2 Interagency Agreement for Placement of a CLETS Terminal	
	1.5.3 Release of Information from the CLETS	
	1.5.4 Reciprocity Agreement	
	1.5.5 Interstate Access	
1.6	<u>SYSTEM RULES</u>	2324
	1.6.1 Database Policies and Regulations	
	1.6.2 Terminal Mnemonics	
	1.6.3 Audits and Inspections	
	1.6.4 Confidentiality of Information from the CLETS	
	1.6.5 Administrative Messages	
	1.6.6 Local/Wide Area Networks – Definition and Requirements	
	1.6.7 Operator Identification Field Requirements	
	1.6.8 Terminal Address Field Requirements	
	1.6.9 Dial-up/Wireless Access to the CLETS	
1.7	<u>SYSTEM DESIGN AND ENHANCEMENT STANDARDS</u>	3334
	1.7.1 Message Switching Computer (MSC) Definition and Requirements	
	1.7.2 MSC Design	
	1.7.3 System Upgrade	
	1.7.4 MSC Test Lines	

<u>SECTION</u>	<u>SUBJECT</u>	<u>PAGE</u>
1.8	<u>TRAINING</u>	36<u>37</u>
	1.8.1 System Training	
	1.8.2 Database Training	
	1.8.3 Security Awareness Training	
1.9	<u>SECURITY</u>	39<u>40</u>
	1.9.1 Location of Terminals and Equipment	
	1.9.2 Background and Fingerprint-Based Criminal Offender Record Information Search	
	1.9.3 User Access	
	1.9.4 Internet Access	
	1.9.5 Logging	
	1.9.6 Encryption	
	1.9.7 Virus Protection	
	1.9.8 Authentication	
	1.9.9 Firewalls	
	1.9.10 Handheld Devices	
	1.9.11 Media Disposal	
	1.9.12 Patch Management	
1.10	<u>SYSTEM DISCIPLINE/APPEAL PROCESS</u>	45<u>46</u>
	1.10.1 System Misuse	
	1.10.2 Discontinuance of CLETS Service	

CLETS POLICIES, PRACTICES and PROCEDURES

SUMMARY

~~This document reflects changes to the February 2009 version of the CLETS Policies, Practices and Procedures (PPP) that were approved by the CLETS Advisory Committee at the March 25, 2010 meeting.~~

~~Only two changes were made to the policies and they are highlighted in the document with **bold** and *italicized* text:~~

~~1.6.1.E.2.b—This section was removed from the PPP. Section 1.6.1.E.2.b previously allowed the California Highway Patrol to use the CLETS to conduct a preliminary criminal offender record information search on applicants for tow truck driver and employers. A legal review of this section determined it was in violation of the *Central Valley versus Younger* decision and subsequent injunctions.~~

~~1.7.3.B—The requirements for an agency's network diagram were updated to correspond with the requirements on the CLETS Application.~~

1.0 LEGISLATIVE INTENT AND LAW

1.0.1 California Government Code – Chapter 2.5

California Government Code (GC) sections 15150 through 15167 state that the California Department of Justice (CA 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 Section 13240) of Chapter 2, Part 3, Division 3, Title 2 of this code, and Chapter 2 (commencing with Section 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 Section 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 Section 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 Department of General 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. 2002, Ch. 545)

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. *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.*

(Added by Stats. 1965, Ch 1595.)

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.*

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 Section 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 Section 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, data bases, 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 Section 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.)

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 of obtaining 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 15161-15163, the CA 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 its 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) 227-3677 Facsimile: (916) 227-0696
E-mail address: CAS@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 work groups 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 The 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 the 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 percent of its annual budget may apply for 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 its annual budget (more than 50 percent) is allocated to the administration of criminal justice.

1.3.2 Applicant Request for Service

Agencies desiring to participate in the CLETS must request an application from the CA DOJ (see PPP section 1.1.3 for address). The application must be submitted through the County Control Agency/Direct Interface System Host.

Routine applications are defined as upgrade applications that meet all PPP requirements and utilize technology previously approved by the CAC. These applications will be approved by the CA DOJ. Any routine application with outstanding issues may be referred to the CAC on a case-by-case basis. 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.

- A. In the event a routine or non-routine application is denied, the CA 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 the CA 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. The CA 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. The CA DOJ shall provide the applicant agency with a written notice of the final decision.

1.3.3. Subscriber Agreement

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

1.3.4 Agency CLETS Coordinator (previously known as the Agency Terminal Coordinator)

Each CLETS subscribing agency must designate an Agency CLETS Coordinator (ACC) who serves as the coordinator with the CA DOJ on matters pertaining to the use of the CLETS, the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC), the National Law Enforcement Telecommunications System (NLETS) and the CA DOJ criminal justice databases and administrative network that the CLETS accesses. The ACC will be responsible for ensuring compliance with the CA DOJ/FBI policies and regulations including validation requirements, as well as facilitate the exchange of the CLETS administrative information between the CA DOJ and the ACC's agency.

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

1.3.5 Security Point of Contact

Pursuant to the FBI's Criminal Justice Information Services (CJIS) Security Policy section 3.4 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 the CA DOJ on security matters pertaining to the use of the CLETS, the NCIC, the NLETS and the CA DOJ criminal justice databases and administrative network that the CLETS accesses. Any information communicated between the CA DOJ and the SPOC will be shared with the agency's ACC.

The SPOC's responsibilities shall be designated by the CA DOJ on a SPOC Responsibilities Form (see **Exhibit K**). If an agency requests other than a permanent, full-time employee as its SPOC, the CA DOJ must be notified in writing and will review the request. Any change in the SPOC's

designation must immediately be provided to the CA DOJ on the Change Request form (see **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 – GC section 15161 requires the CA DOJ 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 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 the CA DOJ for the CLETS, and not hosting other agencies, is referred to as a Local Agency Direct Interface.

1.4.2 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 message switching computer (MSC). It is the responsibility of the County Control Agency/Direct Interface System Host to review all new and upgrade applications to ensure compliance from 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 from 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 the CA 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 continuously is unable to fulfill its responsibilities in providing access, it shall be the responsibility of the CA DOJ in consultation with the 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 will advise the MSC administrator, who will program the MSC for the additional terminals or authorization changes and notify the subscribing agency.

C. Network Security

The link between the County Control Agency/Direct Interface System Host and the CA DOJ is the responsibility of the CA DOJ to manage, maintain and encrypt. The County Control Agency/Direct Interface System Host is responsible for the integrity and security of the network segment that hosts the CLETS 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 CA DOJ and the FBI.

Law enforcement and criminal justice agencies may operate on either trusted or untrusted networks. A trusted network segment is defined as a network used exclusively by law enforcement or criminal justice agencies and managed by those agencies or their designees as set forth in a Management Control Agreement. An untrusted network is defined as a network that may host a combination of law enforcement or criminal justice agencies and non-criminal justice activities/users.

Network segments that host the CLETS message switch/CA DOJ link must be on a trusted network segmented from an untrusted network by a ~~firewall~~ boundary protection device. The ~~firewall~~ boundary protection device shall be controlled by the law enforcement or criminal justice agency or its designee. A minimum ~~firewall~~ boundary protection device profile must be implemented to provide a point of defense, control and audit access to the information from the CLETS as referenced in PPP section 1.9.9.

If an untrusted network will be used to transport the information from the CLETS, the data must be encrypted while in the untrusted network segment. Information from the CLETS traversing a public network shall also be subject to this encryption requirement. Encryption shall meet the minimum requirements as specified in PPP section 1.9.6.

It is incumbent upon the agency to ensure on a regular basis its encryption method meets the minimum-security standards as specified in PPP section 1.9.6.

1.4.3 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 the CA 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 the CA 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 the CA 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 the CLETS service as identified in section 1.3.1 of the CLETS Policies, Practices and Procedures (PPP).
2. Compliance with the CLETS PPP and the FBI's CJIS Security Policy.
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 with 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 the CA DOJ.

B. Upgrade Requirements

When a County Control Agency prepares for an upgrade, the upgrade design must include plans to accommodate all the 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 CLETS Administration Section 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 (see **Exhibit H**).

1.4.4 Direct Interface System Host

A. Role 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 application to the CA DOJ.

The Direct Interface System Host is responsible for providing the CLETS service to the 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 1.4.3.A.

After review of the application, the Direct Interface System Host will attach a letter of intent and forward the completed package to the CA

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 CLETS Administration Section 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 the 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 the CA DOJ.

1.4.5 Local Agency Direct Interface

A. Roles and Responsibilities

Any agency wishing to access the CLETS through a direct interface to the CA DOJ may do so at its own expense and through application to the CA 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 the CA 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 service from other than the normal state-provided interface. This is to include any and all hardware, interface modules and administrative costs incurred by the CA 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 CLETS Administration Section 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 application to the CA DOJ.

1.4.6 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 the CA DOJ within 60 days following the local agency's request. The recommendation shall include one of the following:

1. Recommend approval for immediate access; or
2. Recommend 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 the CA DOJ for review.

1.4.7 Removal of County Control Agency/Direct Interface System Host

In the event it becomes evident to the CA 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 the CLETS service to qualified applicants or users, it shall be the responsibility of the CA 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 responsible criminal justice/law enforcement agency authorized by the CAC.

Copies of the CLETS-related contractual documents must be retained by the ACC of the CLETS subscribing agency for the duration of the life of the document.

1.5.1 Management Control Agreement

A. Public Agency

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

A signed Management Control Agreement must be received by the CA DOJ prior to the CLETS subscribing agency permitting the non-CJ agency access to the 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 (see **Exhibit E**) will also be required.

A non-CJ agency may access the 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 the CA DOJ/FBI criminal justice databases.

The CLETS subscribing agency will maintain responsibility for security control as it relates to the CLETS access. 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 the 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, routers, firewalls boundary protection devices and other components that make up and support a telecommunications network and related CA 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 control includes, but is not limited to, the supervision of applicable equipment, systems design, programming and operating procedures associated with the development, implementation and operation of any MSC 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 that all non-CJ agency personnel accessing the 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 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 an 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 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/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.

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

Exhibit D1 is a sample agreement that meets the CA DOJ and the 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 not inconsistent with the language in Exhibit D1.

B. Private Contractor

The Private Contractor Management Control Agreement (see **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's CJIS Security Addendum (see **Exhibit L**). Vendors with remote access for testing and diagnostic purposes must also enter into a 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 (see **Exhibit E**).
- C. A copy of the statute, ordinance or regulation and the signed Interagency Agreement must be submitted to the CA DOJ for review and approval prior to the placement of a CLETS terminal.
- D. A terminal mnemonic address will be assigned to, and associated with, the CLETS subscribing agency’s Originating Agency Identifier (ORI), and the CLETS subscribing agency assumes full responsibility and liability for all the CLETS activities through the terminal. The receiving agency will be listed as the secondary location for the terminal.
- 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 must complete the required fingerprint-based criminal offender record information search as per PPP section 1.9.2.
- 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 this Interagency Agreement must be submitted to the CA DOJ to review for compliance 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 the CA 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 CLETS PPP, the FBI’s CJIS Security

Policy sections ~~8-0~~ [4.2](#) and ~~6-4~~ [5.1.1.6](#) and the California Code of Regulations, Title 11, Division 1, Chapter 7, Article 1, section 703(b).

If an agency provides information from the CLETS to a non-CLETS subscribing agency a “Release of Information from the CLETS” form (see **Exhibit F**) must be completed. A copy of this Release of Information from the CLETS form must be submitted to the CA DOJ to review for compliance 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 the CA DOJ. In addition to the completion of the form:

- A. All persons having access to information from the CLETS must complete the background and fingerprint-based criminal offender record information search as required per PPP section 1.9.2.
- 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. 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 written agreement or a letter of agreement (see **Exhibit G** for an example of a Reciprocity Agreement). The written agreement or letter of agreement must be signed by the head of each agency and a copy must be submitted to the CA DOJ.

The written agreement or letter of agreement shall be updated when the head of the agency changes or immediately upon request from the CA DOJ.

An agency may request and use Time Activated Message Forwarding (TAMF) if needed in the performance of these functions. (TAMF is further described in Section 2.2 of the CLETS Operating Manual.)

1.5.5 Interstate Access

Pursuant to GC 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 the CA 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 the CA DOJ.

The Interstate Access Agreement shall be updated when the head of the agency changes or immediately upon request from the CA 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 CLETS or the NCIC rules will result in an investigation and appropriate disciplinary action as determined by the CA DOJ in consultation with the CAC.

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. Details of state summary criminal history information may be received by an agency-approved wireless device, provided all wireless access security requirements are met (see PPP section 1.6.9).
- D. Pursuant to the California Code of Regulations, Title 11, Division 1, Chapter 7, Article 1, section 707(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.
- E. The CA DOJ Automated Criminal History System Prohibitions:
 - 1. In reference to U.S. Code, Title 18, Section 922(G)(9), terminals are prohibited from accessing the CA DOJ Automated Criminal History System to enforce the provisions of Title 18 USC 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 the CA 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 sections 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 not to 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 the CA DOJ.
- c. Pursuant to the Code of Civil Procedures section 1279.5(e), the courts shall use the CLETS to determine whether an applicant for a name change is under the jurisdiction of the 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 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. 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 Penal Code Section 13202, access to the DOJ Automated Criminal History System is allowed for law enforcement statistical or research purposes only upon approval by the CA 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 the CA 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 for 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 the CA DOJ.

A subscribing agency that wants to implement mnemonic pooling must submit an application for mnemonic pooling to the CA DOJ for approval. The form and content of the application will be prescribed by the CA 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 section 1.6.7) and the terminal address in the Terminal Address Field (TAF), if provided (see PPP section 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 separate *Mnemonic Pooling Technical Requirements* document for additional technical information about mnemonic pooling.

Each agency must maintain a list of where each terminal is currently located. Such list shall reside with the designated ACC and must be available for the CA DOJ or the FBI inspections. The CA DOJ or the 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 the CA DOJ or the FBI to ensure compliance with CA DOJ/FBI policies and regulations.

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.

Any CLETS accessing agency that also provides Internet access must maintain records of ~~firewall~~ boundary protection security and identify associated CLETS terminal mnemonics. Such records must be made available to the CA DOJ and the FBI during inspections and/or audits.

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. 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 sign an employee statement form prior to operating or having access to the CLETS terminals, equipment or information. This form addresses confidentiality, release and misuse of information from the CLETS (see **Exhibit I** for a sample form.)

- 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. The CLETS terminals and information from the CLETS must remain secure from unauthorized access.
- E. Information from the CLETS may be faxed from one secure location to another secure location. Both the agency faxing the information and the agency receiving the information are responsible for its security.
- F. All information from the CLETS must be stored in a secure and confidential file.
- G. When an agency determines information from the CLETS is no longer needed, the data and/or systems records shall be securely disposed of to prevent access by unauthorized personnel. Such disposal shall include a method sufficient to preclude recognition or reconstruction of data and verification that the procedures were successfully completed. Disposal methods must meet the requirements stated in PPP section 1.9.11.
- H. Information received from a CLETS terminal must be maintained separately from non-law enforcement information.
- I. Terminals must be away from public view with a log-on/log-off, password process in place.

- J. A unique password must be assigned to each CLETS user and must meet the requirements stated in PPP section 1.9.8.
- K. Secondary dissemination and remote access to information from the CLETS using communications media (including the Internet) is allowed when a minimum set of administrative and technical requirements that include encryption and ~~firewall~~ boundary protection requirements as specified in PPP sections 1.9.6 and 1.9.9 is met.

Once information from the CLETS is in the law enforcement or criminal justice agency's network, the agency is directly responsible for maintaining the security and integrity of the data. Any secondary dissemination of the data must be secure and available only to those who are authorized to receive the data. The law enforcement or criminal justice agency must comply with the policies and regulations associated with the release of that data.

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 the CLETS messages direct to the CLETS or through the local MSC. For the 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 the CA 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 work station 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 shall contain the four-to-10 alpha-numeric character supplemental header plus the

extended headers with the OIF (see PPP section 1.6.7) and a TAF, if used (see PPP section 1.6.8).

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.
- E. In an untrusted network, including all public networks (such as wireless, frame relay), those segments that will be used to transport information from the CLETS must:
1. Be segmented from the untrusted portion of the network by a firewall boundary protection device. The firewall boundary protection device shall be controlled by the law enforcement or criminal justice agency or its designee. A minimum firewall boundary protection profile must be implemented to provide a point of defense, control and audit access to information from the CLETS as referenced in PPP section 1.9.9; and
 2. Be encrypted while in the untrusted network segment. Encryption shall meet the minimum requirements as specified in PPP section 1.9.6.

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 as an extension of the four-to-10 alpha-numeric character supplemental header. The OIF is located after the supplemental header, separated by a period, identified by an asterisk, composed of six alpha-numeric characters and terminated by a period.

- 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. Passwords must meet the requirements as stated in PPP section 1.9.8.

- 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 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.
- 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 operator identification information and store the data in the CLETS journal records.
- E. Adequate security controls are required to be maintained over identifiers and passwords.

1.6.8 Terminal Address Field (TAF) Requirements

All MSC, CAD systems and LAN/WAN systems should transmit a TAF. The TAF is a ~~6-~~ 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.

- 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.

1.6.9 Dial-up/Wireless Access to the CLETS

Information from the CLETS is normally transmitted via private, dedicated lines. However, access to the CLETS may be achieved on a public switched line using a dial-up/wireless system upon approval by the CA DOJ. Dial-up/wireless access is allowed from a terminal through its host server or MSC system.

An application for dial-up/wireless access must be submitted to the CA DOJ for approval. The form and content of the application will be prescribed by the CA DOJ. All information and requests should be directed to the address listed in PPP section 1.1.3.

The subscribing agency shall forward the completed application to the County Control Agency/Direct Interface System Host for review and recommendation. The County Control Agency/Direct Interface System Host will forward the application and comments to the CA DOJ for review.

A. Dial-up/Wireless access includes the following:

1. The requesting agency must provide all necessary equipment, such as terminals and modems.
2. Dial-up/Wireless terminals must be identified as such when mnemonics are requested from the CA DOJ. Mnemonics assigned for such purposes must be used only on terminals designated for dial-up/wireless access. The CLETS mnemonics shall not be assigned to vendor terminals.
3. All log-ons, successful and unsuccessful, must be logged. Repeated failed log-on attempts shall disable the user account. All logs must meet the requirements stated in PPP section 1.9.5.
4. Personnel leaving the agency for any reason or no longer authorized access to the CLETS must immediately have their User ID and password deleted by the local agency and host MSC administrator.
5. Dial-up/Wireless terminals must immediately employ, at a minimum, a personal/software-based firewall. Personal firewalls shall meet the requirements stated in PPP section 1.9.9.A. ~~Wireless devices procured before April 30, 2007, do not require a personal/software-based firewall until September 30, 2010.~~

B. All information from the CLETS transmitted using a wireless link or dial-up connection shall be protected with encryption while in that segment.

1. The dial-up/wireless system shall be able to identify and authenticate the user prior to the user gaining access to the CLETS by utilizing a ciphered User ID and password meeting the requirements stated in PPP section 1.9.8 to access the communications server. Encryption shall meet the requirements stated in PPP section 1.9.6.

1.7 SYSTEM DESIGN AND ENHANCEMENT STANDARDS

1.7.1 Message Switching Computer (MSC) Definition and Requirements

A MSC is that portion of the hardware and software solely designed to pass through transactions to and from the CLETS. MSCs shall be maintained with a 98 percent 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 the CA DOJ and the FBI's CJIS Security Policy covering such interfaces.

1.7.2 MSC Design

All MSCs planning to upgrade or relocate must formally advise the CA 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 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 sections 1.4.3 and 1.4.4). The County Control Agency/Direct Interface System Host shall send the application along with comments to the CA 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
- ***the path of all CLETS traffic, both fixed and mobile, from the subscribing agency to the CA DOJ;***
- ***all systems (e.g., Records Management System, CAD, MSC, etc.);***
- ***each individual network (e.g., City, County, etc);***
- ***trusted and untrusted networks (indicate encryption, firewalls boundary protection devices and the controlling agency);***
- ***public network segments used to transport the CLETS traffic;***
- ***Internet access that exists within the network (indicate firewall boundary protection devices and the controlling agency);***
- ***wireless access (e.g., satellite, microwave, wi-fi, cellular, etc.,)***
- ***all points of encryption and decryption;***
- ***remote and dial-up access and by whom it will be accessed (e.g., employee, vendor, etc.)***

- C. An upgrade application submitted by a County Control Agency must include an MSC/Users Costs and Requirements form (see **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 the CA DOJ, the agency must request a test line and any test mnemonics in writing from the CA 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 the CA DOJ.

The CA DOJ will assume line and equipment costs when the system begins production for County Control Agencies only and at such time as the previous CA DOJ provided interface is disconnected. Upon production, the County Control Agency is responsible for sending a letter to the CA DOJ requesting that the test line and test mnemonics be deleted and that charges be transferred to the CA 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 MSC and the use of pre-formatted screens.

1.8.2 Database Training

Training in message formats for access to information in the CA DOJ criminal justice databases, the NCIC, the NLETS, the Department of Motor Vehicles (DMV) and the Oregon Law Enforcement Data System (LEDS) is the responsibility of the CA DOJ. Training will be accomplished according to the following:

- A. It is the responsibility of all city, county, state and federal agencies that use information from the CLETS to participate in the CA DOJ's training programs to ensure all personnel (i.e., terminal operators, peace officers, investigators, clerical, agency management/supervisors, etc.) are trained in the operation, policies and regulations of each file that is accessed or updated. Training shall be provided only by the CA DOJ's training staff or another certified CLETS/NCIC trainer.

Specifically, the training requirements are as follows:

1. Initially (within six months of employment or assignment), 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 the CA DOJ, or a facsimile thereof. An agency wishing to make additions or modifications to the Proficiency Examination must receive prior approval from the CA DOJ.
2. Biennially, 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 the CA DOJ, or a facsimile thereof. An agency wishing to make additions or modifications to the Proficiency Examination must receive prior approval from the CA DOJ.

3. Maintain records of all training, testing and proficiency affirmation. Training records, written or electronic, shall identify the employee'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 biennial Telecommunications Proficiency Examination were completed, recording a passing score of 70 percent 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. An individual's CLETS training record may be deleted one year after separating from the agency.
 4. Initially (within six months of employment or assignment), 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 use 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, the CA 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 CA DOJ staff.

1.8.3 Security Awareness Training

Initially (within six months of employment or assignment), all new employees who have access to the CLETS equipment or information from

the CLETS, including all appropriate Information Technology personnel, shall receive security awareness training and shall meet the requirements specified in the FBI's CJIS Security Policy section 5.2. Thereafter, all personnel who manage or have access to the CLETS equipment or information from the CLETS shall receive security awareness training at a minimum of once every two years. Documentation pertaining to the materials used and those employees who have received security awareness training shall be maintained in a current status.

Documentation of the prior completion of security awareness training may be accepted from another agency. However, accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state or local laws.

1.9 SECURITY

Statewide operational control and system supervision shall be under the direction of the CA DOJ. Monitoring of traffic for conformity to policies, regulations and recommendations for corrective actions shall also be the responsibility of said personnel. The CLETS access is permitted only from an agency-approved device and shall meet the requirements specified in the FBI's CJIS Security Policy sections 5.5.6.1 and 5.5.6.2. Vendors may remotely access the CLETS for testing and diagnostic purposes only and that access will be at the discretion of the agency head.

Agencies with systems interfacing with or to the CLETS shall assist the CA DOJ in overseeing new and upgrade application hardware, software and security of the terminals connected to the computer system for compliance with the CLETS and FBI's CJIS Security policies.

To maintain the integrity of the CLETS and to ensure the security of information received and transmitted by use of the system, the following policies shall be adhered to:

1.9.1. Location of Terminals and Equipment

Pursuant to the FBI's CJIS Security Policy section ~~4.4.1~~ 5.9, reasonable measures shall be taken to locate terminals and equipment in an area with adequate physical security to provide protection from vandalism or sabotage and to preclude access to information from the CLETS by other than authorized personnel. This includes unauthorized viewing or access to computer terminals, access devices or stored/printed data at all times.

Agencies shall immediately notify the CA DOJ of the terminal mnemonic and ORI whenever a terminal is suspected of being stolen or misplaced.

1.9.2 Background and Fingerprint-Based Criminal Offender Record Information Search

A. All persons, including non-criminal justice, volunteer personnel and private vendor technical or maintenance personnel with physical access to the CLETS equipment, information from the CLETS or to criminal offender record information, are required to undergo a background and fingerprint-based criminal offender record information search pursuant to the California Code of Regulations, Title 11, Division 1, Chapter 7, Article 1, Subsections 703(d) and 707(b).

1. Where the CLETS access is available without criminal offender record information, all persons, including non-criminal justice and

private vendor technical or maintenance personnel, accessing areas where the CLETS equipment or information from the CLETS is located are required to undergo a background and fingerprint- based criminal offender record information search.

2. Pursuant to the FBI's CJIS Security Policy section 4.5 [5.12](#), if the 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 that 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 the CLETS access is appropriate.
 3. Visitors to a computer center, such as a tour group where the computer center has criminal offender record information access, are not required to undergo a background and fingerprint-based criminal offender record information search. They must, however, be escorted at all times.
 4. The final responsibility for maintaining the security and confidentiality of criminal justice information rests with the individual agency head or administrator.
- 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 security clearance to include the following checks:
1. A CA DOJ fingerprint-based criminal offender record information search.
 2. An FBI fingerprint-based criminal offender record information search.
 3. Additionally, the CA 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 the CLETS terminals, equipment or information until a background and 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 placed

either in the employee's personnel file or in another pertinent file indicating that authorization has been granted.

Suitability for the CLETS access following the completed background and 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 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. (See **Exhibit I** for a sample Employee/Volunteer Statement Form.)
- B. All log-ins, successful and unsuccessful, must be logged. Repeated failed log-on attempts shall disable the user account and meet the requirements identified in the FBI's CJIS Security Policy section 5.5.3. All logging must meet the requirements stated in PPP section 1.9.5.
- 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 removing all related passwords, security authorizations, tokens, etc., from the system.

1.9.4 Internet Access

- A. Accessing the CLETS directly through the public Internet is prohibited.
- B. Accessing the CLETS from a public Internet connection through a law enforcement or criminal justice agency network is permitted when the following requirements are met:
 - ~~1. A Virtual Private Network (VPN) solution that meets the FBI's CJIS Security Policy section 7.11 shall be used.~~
 - 12. [The transport method, such as a Virtual Private Network \(VPN\), that encryption method](#) meets the encryption requirements as stated in PPP section 1.9.6 shall be used.

3. Two-factor authentication shall be used where at least one factor meets the Advanced Authentication standards identified in the FBI's CJIS Security Policy section ~~7.3.2.3~~ 5.6.2.2.
 4. The VPN communication must pass through a boundary protection device ~~firewall~~ function prior to terminating the VPN session. The boundary protection device ~~firewall~~ must meet the requirements stated in PPP section 1.9.9.
 5. Terminals with the CLETS access shall employ, at a minimum, a personal/software-based firewall. Personal firewalls shall meet the requirements stated in PPP section 1.9.9.
 6. Only agency-owned and/or authorized computer systems shall be used. Personally owned systems shall not be used.
- C. A terminal with the CLETS access shall not access the Internet unless that access is protected by a boundary protection device ~~network firewall~~ that meets the requirements specified in PPP section 1.9.9.

1.9.5 Logging

Pursuant to the FBI's CJIS Security Policy section ~~7.14~~ 5.4, the CLETS terminals and devices used to connect to the CLETS shall, at a minimum, incorporate an audit trail capable of monitoring successful and unsuccessful log-on attempts, file access, type of transaction and password changes. ~~All logging shall meet the requirements specified in the FBI's CJIS Security Policy section 8.4.~~

1.9.6 Encryption

Information from the CLETS and transmitted through any public network segment, wireless network, untrusted network or the public Internet shall be immediately protected with encryption. Information from the CLETS at rest (stored electronically) outside the boundary of the physically secured location shall also be protected with encryption. The encryption shall meet the requirements specified in the FBI's CJIS Security Policy section ~~7.12~~ 5.10.1.2.

Encryption keys used to encrypt information from the CLETS shall be managed through documented procedures detailing key generation, key distribution, key disposal, emergency procedures, key recovery and key escrow. It is the responsibility of the law enforcement or criminal justice agency or its designee to document and keep current all encryption key management practices.

1.9.7 Virus, Malicious Code, Spam and Spyware Protection

All systems with the CLETS connectivity or access to information from the CLETS shall employ virus, spam and spyware protection software that meets the requirements stated in the FBI's CJIS Security Policy section ~~7.15~~ 5.10.4.2 and 5.10.4.3.

1.9.8 Authentication

Each person authorized to store, process and/or transmit information from the CLETS shall be uniquely authenticated prior to access to the CLETS.

- A. Where passwords are used to authenticate users, those passwords shall meet the requirements stated in the FBI's CJIS Security Policy section ~~7.3.3~~ 5.6.2.1.
- B. Where advanced authentication is required (such as receiving information from the CLETS over the Internet), the advanced authentication shall meet one of the approved methods as described in the FBI's CJIS Security Policy section ~~7.3.2.3~~ 5.6.2.2.

1.9.9 Firewalls Boundary Protection

The information between interconnected systems must be controlled to regulate where information is allowed to travel within an information system and between information systems without explicit regard to subsequent access to that information. Specific examples of flow control enforcement can be found in boundary protection devices such as firewalls, encrypted tunnels and routers that employ rule sets or establish configuration settings that restrict information system services or provide packet filtering capabilities. Firewalls Boundary protection devices are implemented to provide a point of defense, control and audit access to the CLETS equipment and information from the CLETS. Where firewalls boundary protection devices are required, those firewalls devices shall meet the requirements as stated in the FBI's CJIS Security Policy section ~~7.13~~ 5.10.1.

A. Personal Firewalls

A personal firewall is defined as a firewall that can operate with only one network interface. Personal firewalls are required for ~~wireless~~ all mobile devices and shall meet the requirements specified in the FBI's CJIS Security Policy section ~~7.13.3~~ 5.10.4.4.

1.9.10 Handheld Devices

Handheld devices used are permitted to receive information from the CLETS ~~are permitted if the following additional requirements are met~~ when the requirements specified in the FBI's CJIS Security Policy section 5.5.7.3.1 are met. The handheld devices referenced here include, but are not limited to, Personal Digital Assistants, Personal Electronic Devices, cellular phones, smart phones and other multifunction handheld devices.

- ~~A. A handheld device shall incorporate a personal firewall. A personal firewall is defined as a firewall that can operate with only one network interface on a personal computer or other handheld computing device. Personal firewalls shall meet the requirements specified in the FBI's CJIS Security Policy section 7.13.3.~~
- ~~B. Information from the CLETS shall not be stored unprotected on handheld or portable media devices. Information from the CLETS stored on handheld or portable media devices shall have all residual data protected by encryption or erasure. Encryption shall meet the requirements stated in PPP section 1.9.4.~~

1.9.11 Media Disposal

When no longer usable, diskettes, tape cartridges, ribbons, hard copies, printouts, compact disks, digital versatile disks and other similar items used to process and store information from the CLETS shall be destroyed. Destruction methods shall meet the requirements stated in the FBI's CJIS Security Policy section 4.6 5.8.4.

1.9.12 Patch Management

All systems and devices with connectivity to the CLETS or access to information from the CLETS shall use manufacturer-supported software and firmware. Critical security shall be fully tested and installed immediately upon release from the manufacturer. ~~Exceptions to this requirement shall be submitted to the CA DOJ and reported on at the CAG meetings~~ in accordance to the requirements stated in the FBI's CJIS Security Policy section 5.10.4.1.

1.10 SYSTEM DISCIPLINE/APPEAL PROCESS

Pursuant to CG 15154, the CA DOJ is responsible for overseeing system discipline with the assistance of the CAC. Messages/transactions processed through the CLETS shall be subject to random sampling by the CA DOJ, or its designee(s), for validity of content and conformity with CLETS policies and regulations.

1.10.1 System Misuse

- A. Violation of the CLETS policies, practices and procedures shall be investigated by the agency head or his/her designee and reported to the CA DOJ.

The agency head or his/her designee shall investigate the incident of system abuse by reviewing its internal processes and documentation. In the event the agency head requires assistance from the CA 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 the CA 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 the CA DOJ.

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

If the reported explanation and corrective actions do not resolve the problem to the satisfaction of the CA 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. The CA DOJ will issue a letter formally notifying the agency of the decision.

- B. In the event of a violation of law or CLETS policies, practices and procedures result in system misuse, the CA DOJ with a recommendation from the CAC will take appropriate action such as:
 - 1. Letter of censure;

2. Suspension of service – 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.
- 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 the CA DOJ on the number of investigations performed related to the CLETS misuse, and any disciplinary action taken. This report will be submitted by February 1 of each year for the preceding calendar year. This information will be submitted on the CLETS Misuse Investigation Reporting Form (reference **Exhibit J**).

1.10.2 Discontinuance of the CLETS Service

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

