CLETS POLICIES, PRACTICES and PROCEDURES

Table of Contents

CLETS POLICIES, PRACTICES and PROCEDURES

EXECUTIVE SUMMARY -- POLICY CHANGES

Changes approved at the most recent CLETS Advisory Committee meeting are reflected in the body of this document.

The following sections have been affected and the changes are summarized below. Be sure to refer to each specific section within the PPPs to read the complete detail of the revisions.

October 29, 2008

1.6.4.K Language was modified to refer to the FBI's CJIS Security Policy for encryption and firewall requirements.

1.9.4 Language was modified to refer to the FBI's CJIS Security Policy for encryption and firewall requirements.

June 25, 2008

1.6.4.K Language from 1.9.4 was moved to this section and modified to allow the secondary dissemination of data accessed via the CLETS when requirements are met.

1.9.4 Language was modified to allow CLETS access via the Internet when requirements are met.

June 14, 2005

1.3.5 Language was added to establish a Security Point of Contact (SPOC) position within each CLETS subscribing agency.

1.4.6 Language was added to establish the requirement for CLETS host agencies to encrypt CLETS data over public networks.

1.5.1.B Language was added to establish the requirement for a Management Control Agreement (MCA) for use with private contractors. There was also a section reference change for the existing MCA for use with a public agency.

1.6.1.C.3 Language was removed that disallowed ACHS transmissions over wireless segments for routine traffic.

1.6.2 Language was modified to require a 90-day notice prior to deletion of mnemonics inactive for nine months. Language allowing for an appeal was removed.

1.6.6.E.2 Language was added to establish the requirement for CLETS data to be encrypted over public networks when using a LAN/WAN.

1.6.9.B Language was added to establish the requirement for CLETS data to be encrypted over public networks when using a dial-up/wireless system.

1.0 LEGISLATIVE INTENT AND LAW

1.0.1 California Government Code – Chapter 2.5

Chapter 2.5, Section 15150 through 15167, California Government Code states that the Department of Justice 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 Local, State and Federal Government

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.

1.1.2 Purpose of CLETS

The California Law Enforcement Telecommunications System (CLETS) will provide all law enforcement user agencies with the capability of obtaining information directly from federal, state and local computerized information files. In addition, the system will provide fast and efficient point to point delivery of messages between agencies.

1.1.3 State Provided Services

CLETS is a cooperative service whereby the State provides central switching equipment, personnel to staff the switching center, and sufficient circuitry from the switching center to such locations as authorized by law (<u>one</u> location in <u>each county</u>) 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.

1.1.4 Request for General Information

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

CLETS Executive Secretary
Department of Justice
P.O. Box 903387
Sacramento, CA 94203-3870
Telephone (916) 227-3677, FAX (916) 227-0696

1.2 CLETS ADVISORY COMMITTEE (CAC)

1.2.1 Responsibilities of Committee

The responsibilities of the CLETS Advisory Committee are defined in California Government Code Sections 15154 through 15167.

1.2.2 Subcommittees

The chairperson of the CLETS Advisory Committee may appoint subcommittees and/or work groups to consider the CLETS user qualifications, operating rules, policies and practices, and other matters as appropriate.

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

1.2.3 Committee Member Consultation

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

1.2.4 Alternate Members

Any member who is unable to attend a meeting can, with prior approval of the chairperson, send an alternate as a representative. The alternate cannot vote on policy matters or applications for CLETS service.

1.3 QUALIFICATIONS FOR MEMBERSHIP IN CLETS

1.3.1 Eligibility for CLETS Service

The California Government Code 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 which performs law enforcement or criminal justice functions pursuant to a statute or executive order, and to which it appropriates more than fifty percent of its annual budget may apply for CLETS service. Participating agencies in CLETS are referred to as Class I-Law Enforcement, Class II-Criminal Justice or Class III-other types of law enforcement agencies. The CLETS Advisory Committee will establish priority access to CLETS.

A. A Class I law enforcement subscriber is defined as a public agency having statutory powers of arrest and whose primary function is that of apprehension and detection. Class I users include, but are not limited to, sheriffs, city police departments, California Highway Patrol, Department of Justice, and the Federal Bureau of Investigation.

B. A Class II criminal justice agency is a public agency performing a criminal justice function other than apprehension. Class II subscribers include agencies devoted to the administration of criminal justice with personnel whose primary purpose is detention, pretrial release, post trial release, prosecution, adjudication, correctional supervision, rehabilitation of accused persons or criminal offenders, criminal identification activities, and the collection, storage and dissemination of criminal history record information. Agencies include, but are not limited to, district attorneys, courts, probation departments, and other miscellaneous local, state and federal agencies performing such functions.

C. A Class III subscriber is the sub-unit of a non-law enforcement public agency which performs the duties of a law enforcement agency, and whose employees are peace officers. Examples of Class III agencies include Department of Insurance -- Fraud Division, Employment Development Department - Investigations Bureau, university, college and school district police departments, and any fire department - arson investigation unit.

1.3.2 Applicant Request for Service

All agencies desiring to participate in the CLETS system must request an application in writing from the CLETS Executive Secretary (See Section 1.1.4 for address). The application must be submitted through the county control agency/direct interface system host to the CLETS Executive Secretary for consideration by the CLETS Advisory Committee.

Prior to approval by the CLETS Advisory Committee (CAC), agencies expressing a need may be granted temporary connection to CLETS. This temporary access would be granted if approved by the CAC Chairperson, and if all qualifying requirements are met. Any violations of the *CLETS Policies, Practices, and Procedures* by an agency with temporary access to CLETS would be grounds for immediate termination of CLETS service.

1.3.3 Subscriber Agreement

All agencies participating in CLETS must file a Subscriber Agreement signed by the agency head with the Attorney General through the CLETS Executive Secretary as required by California Government Code Section 15165. A new Subscriber Agreement **(reference Exhibit A)** shall be updated at least every three years, when the head of the agency changes, or immediately upon request from the CLETS Executive Secretary.

1.3.4 Agency Terminal Coordinator

Each CLETS subscribing agency must designate an Agency Terminal Coordinator (ATC). The ATC is the key person chosen to serve as the coordinator with the Department of Justice (DOJ) on matters pertaining to the use of CLETS, NCIC, NLETS, and the DOJ criminal justice databases and administrative network that CLETS supports. The ATC will facilitate the exchange of CLETS information between DOJ and the ATC's agency.

The ATC must be a permanent, full-time employee, and cannot be a vendor, consultant, or any other non-law enforcement or non-criminal justice personnel. ATC responsibilities shall be designated by DOJ. DOJ must be notified immediately of a change in ATC designation **(reference Exhibit B, Change Request Form and Exhibit C, ATC Responsibilities Form**).

1.3.5 Security Points of Contact

Each CLETS subscribing agency must designate a Security Point of Contact (SPOC). The SPOC is the key person chosen to serve as the security coordinator with the Department of Justice (DOJ) on security matters pertaining to the use of CLETS, NCIC, NLETS, and the DOJ criminal justice databases and administrative network that CLETS supports. Any information communicated between DOJ and the SPOC will be shared with the agency's ATC.

The SPOC may be a permanent, full-time employee; vendor; or consultant. SPOC responsibilities shall be designated by DOJ. DOJ must be notified immediately of a change in the SPOC designation.

1.4 CLETS DIRECT INTERFACE RESPONSIBILITIES

Section 15161 of Chapter 2.5 of the Government Code of the State of California requires that the Department of Justice 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. Exceptions to this policy may be presented to the CLETS Executive Secretary for consideration by the CLETS Advisory Committee.

1.4.1 County Control Agency

Section 15163 of the California Government Code requires that the system shall provide service to any law enforcement agency qualified by the CLETS Advisory Committee which, at its own expense, desires connection through the county control agency's facility.

In order 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 point of entry into the county. The County Sheriff will serve as County Control Agent unless, by recommendation of the CLETS Advisory Committee to the Attorney General, there exists another law enforcement agency in the county better qualified to act as control agency.

The County Control Agency is responsible for providing CLETS message switching computer (MSC) service to all requesting CLETS subscriber agencies within each respective county. The cost of that service to local agencies should not reflect more than the actual costs attributed to the MSC functionality, including any and all hardware, software, interface modules, and administrative costs incurred by the County Control Agency. If the County Control Agency cannot accommodate a CLETS subscriber's needs, the County Control Agency shall provide the subscriber with written approval to pursue a CLETS connection through other means. "Other means" shall include a connection to CLETS through another hosting MSC or a direct connect to CLETS at the requesting agency's expense.

When a County Control Agency prepares for an upgrade, the upgraded design must include plans to accommodate all CLETS agencies with approved access behind the County MSC, projected new terminals, and future CLETS subscriber agencies.

It is the County Control Agency's responsibility to keep the CLETS Executive Secretary and all affected CLETS subscriber agencies informed in writing of any changes to the county MSC.

1.4.2 Local Agency Direct Interface

A. Local agencies approved for CLETS service may access CLETS through the County Control Agency, a Direct Interface System Host, or by connecting directly to the Department of Justice. Any CLETS subscribing agency wishing to access CLETS through a direct interface to the Department of Justice must:

1. Send a written request to the CLETS Executive Secretary for an application for direct access.

2. Provide written notification, no less than 60 days, to the current County Control Agency or Direct Interface System Host advising them of the plans to change hosting MSC, including projected dates.

3. Forward the completed application for direct CLETS service to the CLETS Executive Secretary. The completed application also should include:

   a. A copy of the letter of notification made to the current hosting agency.

   b. A written justification for the direct interface. The justification should include at least one of the following:

      1. The interface facilities at the termination point in the resident county are inadequate to add and support the applicant.

      2. The termination point in the resident county cannot accommodate the applicant due to degraded service; e.g., a minimum of 98% up time cannot be maintained, the host system is less sophisticated than the applicant's system, etc.

   c. Special justification requests will be reviewed on a case-by-case basis.

   d. A letter of agreement from the applicant's current CLETS access host. The letter of agreement will state the applicant's access to CLETS will continue through that system or another host MSC until applicant obtains and initiates direct access.

4. Provide 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 Department of Justice to provide any direct interface capability.

B. Once a local agency has been approved for direct access, it is their responsibility to keep the CLETS Executive Secretary and all affected CLETS subscriber agencies informed in writing of any changes to the local CLETS computer interface.

1. Upgrades to a local agency's existing direct interface computer system to CLETS must be approved through application to the CLETS Executive Secretary on behalf of the CLETS Advisory Committee.

2. All requests for system changes must be submitted on a "Terminal Access Request Form" from the direct interface MSC administrator to the CLETS Executive Secretary. Once the changes have been implemented, the CLETS Executive Secretary will provide a written response to the direct interface MSC control person.

1.4.3 Direct Interface System Host

A local agency with a direct interface to CLETS may provide a CLETS interface for police departments. Agencies wishing to act in the capacity of a Direct Interface System Host do so at their own expense and through application to the CLETS Advisory Committee.

A. Any police department desiring to access CLETS through a Direct Interface System Host must:

1. Send a written request to the CLETS Executive Secretary for an application to upgrade service.

2. Provide written notification, no less than 60 days, to the current County Control Agency advising them of the plans to change hosting MSC, including projected dates.

3. Forward the completed application to the Direct Interface System Host. The Direct Interface System Host will review the application, attach a letter of intent to provide service, and forward the completed package to the CLETS Executive Secretary. The completed application should also include a copy of the letter of notification made to the existing hosting MSC.

B. The Direct Interface System Host is responsible for providing CLETS message switching computer (MSC) service to all CLETS subscribing agencies hosted behind their system. The cost for services provided by the host agency to a local agency will be by agreement between the involved agencies. Determination of whether to host an agency will be at the sole discretion of the Direct Interface System Host.

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

D. If a hosted 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 through the CLETS Executive Secretary.

E. When a Direct Interface System Host agency prepares for an upgrade, the upgraded design must include plans to accommodate all CLETS subscribing agencies with approved access behind the host MSC, projected new terminals, and future CLETS subscriber agencies.

F. It is the Direct Interface System Host agency's responsibility to keep the CLETS Executive Secretary and all affected CLETS subscriber agencies informed in writing of any changes to the host MSC.

1.4.4 Local Agency Petitioning to Forego Direct Interface and Appeals

A. A local agency with a direct CLETS computer interface or connection to a non-county host MSC wishing to forego such access and return to the resident county CLETS connection must send a written request to the County Control Agency and through the CLETS Executive Secretary to the CLETS Advisory Committee. The County Control Agency must provide a written recommendation within sixty days following the local agency's request. The recommendation shall include one of the following:

1. Recommend approval for immediate access.

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 message switching service through the county host system will be considered applicable.

B. Direct Access Appeals

If a local agency petitioning to forego a direct interface to CLETS or connection to a non-county host MSC is unable to gain access to the County MSC, per Section 1.4.4.A, the matter will be referred to the CLETS Advisory Committee.

A CLETS Ad-hoc Review Committee shall be convened in accordance with Section 1.4.4.C to review the matter and make recommendations to the CLETS Advisory Committee.

C. Formulation of an Ad-hoc Review Committee

An Ad-hoc Review Committee shall be convened by the CLETS Advisory Committee (CAC) Chairperson. Its function shall be solely to review and make recommendations on local agency application to a county MSC when relinquishing a direct interface or non-county host MSC connection to CLETS when such matters are referred to them for consideration by the CLETS Executive Secretary. Such recommendations shall be provided to the CLETS Advisory Committee.

The CAC Chairperson shall convene an Ad-hoc Review Committee from that portion of the state where the applicant resides. Each committee shall consist of five persons representing all points of view, to include at least one sheriff's representative and one police department representative. They will serve at their own expense. The CAC Chairperson will act as a non-voting chairperson. The DOJ CLETS Administration Section shall provide a non-voting staff support person to the committee.

1.4.5 Application Review

The County Control Agency or Direct Interface System Host will act as the first level of review for all new and upgrade applications for CLETS service provided by the host system's Message Switching Computer (MSC).

A. The review of an application for new service must determine the following:

1. The applicant is a law enforcement or criminal justice agency or other public agency authorized to receive CLETS service as defined in Section 1.3 of the *CLETS Policies, Practices, and Procedures*.

2. A need for CLETS service exists to support the normal activities of the applicant.

3. A County Control Agency must also determine if facilities, such as hardware ports or digital sending units, and the physical computer room space are available at the CLETS point of entry into the county 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.

B. The review of an application for upgrade of service must determine the following:

1. The County Control Agency/Direct Interface System Host has adequate technology to accommodate the upgrade of service.

2. The County Control Agency/Direct Interface System Host MSC can maintain a 98% uptime as defined in Section 1.7.1 once the upgraded system is in production.

C. Positive findings in all of these determinations will provide grounds for concurrence with the application.

D. Negative findings in any of these determinations may be grounds for withholding concurrence.

E. In either event, County Control Agency/Direct Interface System Host comments shall be addressed to the CLETS Advisory Committee through its CLETS Executive Secretary. The CLETS Executive Secretary will review and submit the completed application to the CLETS Advisory Committee for approval. Changes to the application should be in writing.

1.4.6 County Control Agency/Direct Interface System Host Requirements

The County Control Agency/Direct Interface System Host establishes the requirements for access through their MSC and must inform its users of the following:

A. The type of circuitry and equipment necessary for access and how it can be obtained.

B. The type of services provided from the host MSC in addition to CLETS access, such as countywide databases or dispatching.

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

D. Type of video display screen options.

The CLETS host agency is responsible for the integrity and security of the network segment which hosts the CLETS message switch. Law enforcement/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/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/criminal justice agencies and non-criminal justice activities/users.

Network segments which host the CLETS message switch/DOJ link must be on a trusted network segmented from an untrusted network by a firewall. The firewall shall be controlled by the law enforcement/criminal justice agency or their designee. A minimum firewall profile must be implemented to provide a point of defense, control, and audit access to CLETS data as referenced in Section 1.9.4. Information on minimum firewall profiles can be found at the following websites: www.certicom.com and www.trusecure.com.

If an untrusted network will be used to transport the CLETS data, the CLETS data must be encrypted while in the untrusted network segment. CLETS data traversing a public network shall also be subject to this encryption requirement. A public network, whether it is trusted or untrusted, is defined as a common carrier ATM or Frame Relay network where by virtue of their design, the redundancy that is provided, is done so through the use of shared public switches within the network cloud. Agencies initiating use of a public network must comply at the time of implementation with the minimum-security standards as specified in the CLETS Technical Guide. Agencies already approved for utilizing a public network to access CLETS on that date must be in compliance with these standards prior to June 2008.

It is incumbent upon the agency to ensure on a regular basis that their encryption method meets the minimum-security standards as specified in the CLETS Technical Guide.

1.4.7 Host System Training

The County Control Agency/Direct Interface System Host is required to train its host system users in the following areas:

A. How to utilize CLETS and associated databases via the hosting MSC to CLETS.

B. How to use pre-formatted screens, if provided by the host system.

1.4.8 Access Authorization Requests

The County Control Agency or direct interface system host will request additional terminal mnemonics or changes to database authorizations for all users behind their system.

A. The requesting agency must submit a complete "Terminal Access Request Form" to the respective direct interface MSC.

B. The MSC administrator will review the request to ensure it can be accommodated by the MSC, sign the request, and forward it to the CLETS Executive Secretary for processing.

C. Upon completion of the CLETS terminal authorization changes, the CLETS Executive Secretary will advise the MSC administrator, who will program the MSC for the additional terminals or authorization changes and notify the requesting agency.

1.4.9 Removal of County Control Agency/Direct Interface System Host

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

1.5 CONTRACTUAL AGREEMENTS

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

Copies of CLETS-related contractual documents must be retained by the ATC 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 an agreement required when a public law enforcement or criminal justice agency (referred to as the *CLETS subscribing agency*) allows authorized 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 CLETS Executive Secretary prior to the CLETS subscribing agency permitting the non-CJ agency access to CLETS. If a terminal will be placed at a location other than the subscribing agency, an Interagency Agreement will also be required.

A CLETS subscribing agency may delegate the responsibility of dispatching, parking citation, or data processing/information technology services to a non-CJ agency. The non-CJ agency may access information obtained via CLETS on behalf of the CLETS subscribing agency in order to accomplish the above-specified services, if such delegation is authorized pursuant to Executive Order, statute, regulation, or interagency agreement.

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.

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:

A. Standards for the selection, supervision, and termination of personnel. This does not grant hiring/firing authority to the CLETS subscribing agency, only the authority to grant CLETS systems access to personnel who meet these standards and deny it to those who do not; and

B. Policies governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that make up and support a telecommunications network and related CJIS systems 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 computerized message-switching or database systems utilized by the served public law enforcement 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 CLETS information meet the minimum background, training, and certification requirements which 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 CLETS-obtained information. The minimum requirements include, but are not limited to:

C. State and FBI fingerprint-based record checks must be conducted prior to allowing access to CLETS computers, equipment, or information. If the results of the fingerprint-based check reveals a record of any kind, access will not be granted until the CLETS subscribing agency can review the matter to decide if access is appropriate. If a felony conviction of any kind is found, access shall not be granted.

D. Each individual must sign an Employee/Volunteer Statement Form prior to operating or having access to CLETS computers, equipment, or information.

E. 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 1.8.3.

   The CLETS subscribing agency has the responsibility and authority to monitor, audit, and enforce the implementation of this agreement by the non-CJ agency. The non-CJ agency agrees to cooperate with the CLETS subscribing agency in the implementation of this agreement, and to accomplish the directives for service under the provisions of this agreement.

Information obtained via CLETS is confidential and may 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 at least every three years, when the head of either agency changes, or immediately upon request from the CLETS Executive Secretary.

Exhibit D is a sample agreement which has been approved by the CLETS Advisory Committee and NCIC in regard to its policy. A management control agreement which 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 D.

B. Private Contractor

The Private Contractor Management Control Agreement is required when a CLETS subscribing agency allows CLETS access or access to record storage areas containing CLETS-obtained information 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 authorized access to CLETS or CLETS-obtained information must abide by NCIC's CJIS Security Addendum. 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 CLETS may place a CLETS terminal with a governmental agency only under the following conditions:

A. A statute, ordinance, or regulation must exist which requires the governmental agency to perform a law enforcement-related function which necessitates access to DOJ/CLETS provided information.

B. The heads of both agencies must sign an interagency agreement which states that all CLETS rules, regulations, policies, practices, and procedures will be adhered to by all parties involved **(reference Exhibit E)**.

C. A copy of the statute, ordinance, or regulation and the signed interagency agreement must be submitted to the CLETS Executive Secretary 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 CLETS activity 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 DOJ/CLETS provided information must complete the required background check per Section 1.9.2.

G. 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 can only be provided by the CLETS subscribing agency's certified CLETS/NCIC trainer, and must meet all CLETS training requirements per Section 1.8.3.

H. A CLETS subscribing agency may not place a terminal with another agency that meets eligibility requirements for CLETS service as a Class I, Class II, or Class III agency per Section 1.3.1. Such an agency must complete an application for new CLETS service.

I. A copy of this interagency agreement must be submitted to the CLETS Executive Secretary to review for compliance and retention in the CLETS subscribing agency's file. The interagency agreement shall be updated at least every three years, when the head of the agency changes, or immediately upon request from the CLETS Executive Secretary.

1.5.3 Release of CLETS Information

The release of CLETS provided information from a CLETS subscribing agency is authorized on a need-to-know, right-to-know basis and under the following conditions

A. A statute, ordinance or regulation must exist which authorizes the governmental agency to perform a specific function which necessitates access to DOJ/CLETS provided information.

B. An agency wishing to provide CLETS delivered information to a non-CLETS subscribing agency must complete a "Release of CLETS Information" form **(reference Exhibit F)**.

1. All persons having access to DOJ/CLETS provided information must complete the required background check per Section 1.9.2.

2. 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 Section 1.8.3.

3. All subsequent requests for information by an agency with a current "Release of CLETS Information" form on file will be covered.

4. The Release of CLETS Information form shall be updated at least every three years, when the head of the agency changes, or immediately upon request from the CLETS Executive Secretary.

   A copy of this Release of CLETS Information form must be submitted to the CLETS Executive Secretary to review for compliance and retention in the participant's file.

1.5.4 Reciprocity Agreement

Any agency which agrees to perform record entry/update and/or hit confirmation functions on behalf of another agency must enter into a written agreement **(reference Exhibit G)**. This Reciprocity Agreement must be signed by the head of each agency.

A Reciprocity Agreement entered into by two agencies must incorporate the exact wording of the sample agreement, but may be expanded to meet other requirements of the participating agencies. The Reciprocity Agreement shall be updated at least every three years, when the head of the agency changes, or immediately upon request from the CLETS Executive Secretary.

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

Per California Government Code Section 15162, CLETS may connect and exchange traffic with compatible systems of adjacent states and otherwise

participate in interstate operations. Adjacent state agencies subscribing to CLETS must adhere to all CLETS rules, regulations, policies, practices, and procedures.

An Interstate Access Agreement must be completed and submitted to the CLETS Executive Secretary 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 California Attorney General or his/her designee.

The Interstate Access Agreement shall be updated at least every three years, when the head of the agency changes, or immediately upon request from the CLETS Executive Secretary.

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 CLETS. Violations of CLETS rules will result in an investigation and appropriate disciplinary action as determined by the CLETS Advisory Committee.

1.6.1 Database Regulations

All users shall abide by all regulations pertaining to the data obtained from databases accessed through 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 CLETS subscribing agency employees where driving is a requirement of their job.

NOTE: Home address information must remain in the employee's personnel file and may not be disclosed for any reason. (See California Vehicle Code Section 1808.45)

C. DOJ Automated Criminal History System Prohibitions:

1. In reference to US Code, Title 18, Section 922(G)(9), terminals are prohibited from accessing the DOJ Automated Criminal History System to enforce provisions effecting a lifetime firearms or ammunition prohibition for anyone convicted of a "misdemeanor crime for domestic violence."

2. Terminals are not authorized to access automated California Criminal Offender Record Information (CORI) through CLETS for licensing, certification, or employment purposes, including pre-employment background investigations for sworn peace officers and/or law enforcement employees as specified in 830 P.C. et al; or for remotely accessing a record for review and/or challenge by the subject of a record.

   Exceptions:

   a. Per Education Code Sections 45125.5 and 35021.1, a law enforcement agency may agree to provide a school district or county office of education an automated records check of a prospective

non-certificated employee or non-teaching volunteer aide. If the law enforcement agency agrees to provide the automated record check, 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. Per Vehicle Code, Section 2431, the California Highway Patrol may utilize CLETS to conduct preliminary criminal history checks on applicants for tow truck driver and owner/driver certificates.

c. Section 11105.03 of the Penal Code **allows** a law enforcement agency to furnish specific summary criminal history information to a regional, county, city, or other local public housing authority for screening prospective participants as well as potential and current staff. The only criminal history information which can be released must be related to adult convictions for specific felonies or a domestic violence offense. The applicable findings shall be released directly to the housing authority, unless the subject is on probation or parole. In applicable cases, the information shall also be released to the probation or parole officer. Reference PC Section 11105.03 for specifics. 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 CLETS Advisory Committee.

d. Per the Code of Civil Procedures, Section 1279.5(e), the courts shall use CLETS to determine whether or not an applicant for a name change is under the jurisdiction of the Department of Corrections or is required to register as a sex offender pursuant to Section 290 of the California Penal Code. If a court is not equipped with CLETS, the clerk of the court shall contact an appropriate local law enforcement agency which shall determine whether or not the applicant is under the jurisdiction of the Department of Corrections or is required to register as a sex offender pursuant to Section 290 of the Penal Code.

e. Per Section 11105.6 of the Penal Code, a law enforcement agency may access state summary criminal history information via CLETS to notify bail agents if a fugitive has been convicted of a violent felony. Reference PC Section 11105.6 for specifics.

f. Pursuant to Sections 309 and 361.4, and 16504.5 of the Welfare and Institutions Code, county child welfare agency personnel conducting

an assessment for the placement of a child are entitled to state summary criminal history information obtained through 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.

g. CLETS may be accessed to conduct background investigations of candidates for appointment as private, **non-professional** guardians or conservators.

D. DOJ Automated Criminal History System allowances:

1. Details of summary criminal history may be received by an agency approved wireless device, provided all wireless access security requirements are met (see Section 1.6.9). Justification records must be maintained as described in Section 1.6.1.E.

2. Staff of any law enforcement or correctional/detention facility may process on-line criminal history inquiries on any visitor to such facility.

3. A preliminary records check may be performed on any person prior to their approval as a "ride-along" with a law enforcement officer, provided that person is not an employee of the law enforcement agency.

4. 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 Director of the Department of Justice, Division of California Justice Information Services.

E. Section 707 (c) of the California Code of Regulations requires every agency to keep a record of all inquiries into the Criminal History System (CHS) for a minimum of three years with justification of the "need to know" and "right to know," and any subsequent third party dissemination of that information.

F. Test records are available for each database. Refer to the *CJIS Manual*, *DMV Manual for CLETS* and the *NCIC Operating Manual* for test records. Active records shall not be used to test a system or train employees.

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 Class I 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 CLETS Executive Secretary. Message traffic for that terminal must directly terminate at a printer and not to a queue. All fixed CLETS terminals receiving hit confirmation requests or locate messages must directly terminate such messages at a printer and not to a queue. 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 CLETS Advisory Committee.

A subscribing agency that wants to implement mnemonic pooling must submit an application for mnemonic pooling through the CLETS Executive Secretary to the CLETS Advisory Committee for approval. The form and content of the application will be prescribed by the Department of Justice. All information and requests should be directed to the address listed in section 1.1.4.

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. ACP's 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. ACP's 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; determination of how all traffic was handled; determination of when, by date and time, all traffic receipts and deliveries occurred; and who 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 section 1.6.7) and the terminal address in the Terminal Address Field, if provided (see 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 Agency Terminal Coordinator, and must be available for CLETS inspections. Department of Justice staff must be allowed access to any CLETS terminal at any time for audits or other on-site inspections.

Any terminal mnemonic which remains inactive for 9 months will be deleted from 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 Department of Justice or NCIC to ensure compliance with CLETS/NCIC rules, regulations, policies, practices, and procedures.

Authorized personnel performing inspections or audits shall have access to review and/or inspect case files and any records identified in the inspection/audit process, excluding active investigations or cases. The agency being inspected shall produce such records.

1.6.4 Confidentiality of CLETS Messages

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

It is required that each employee/volunteer sign an employee statement form prior to operating or having access to CLETS terminals, equipment, or

information. This form addresses confidentiality, release, and misuse of CLETS information. (See Exhibit I for a sample form.)

A. Access to CLETS information 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 CLETS information for non-law enforcement purposes is prohibited, unless otherwise mandated, and is subject to administrative action and/or criminal prosecution.

D. CLETS terminals and information must remain secure from unauthorized access.

E. CLETS-provided information 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 CLETS information retained must be stored in a secure and confidential file.

G. When an agency determines CLETS information is no longer needed, the information 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 information and verification that the procedures were successfully completed. (Examples may include: shredding paper documents; drilling holes into optical disks, performing format conversion on fixed disks, and degaussing magnetic tapes.

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.

K. Secondary dissemination and remote access to data accessed via the CLETS using communications media (including the Internet) is allowed when a minimum set of administrative and technical requirements that include encryption and firewall requirements as specified in the FBI's CJIS Security Policy sections 7.8 and 7.10 are met.

Once data accessed via 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 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. Any message of excessive length will be reviewed for conformity to CLETS rules. Messages must conform to the examples illustrated in Chapter 2, Message Types, and in Chapter 7, All Points Bulletins (APB), of the *CLETS Operating Manual*. CLETS subscribers should transmit administrative messages or all points bulletins one time only, unless additional pertinent information is obtained and must be relayed.

A. Example of messages acceptable for transmission over CLETS include, but are not limited to:

   1. Requests for record validation.

   2. Information regarding the circumstances surrounding the death of an officer killed in the line of duty, and related funeral notice.

   3. Requests for prisoner pickup and transportation.

   4. Requests for mail-back information from databases.

   5. Notices such as law enforcement related meetings and training and seminar announcements.

   6. Stolen identification cards/badges. (When possible, this information should be entered into the Automated Property System.)

   7. Lost law enforcement identification cards/badges.

B. Examples of messages not acceptable for transmission over CLETS include:

   1. Notices such as social functions, general funeral notices, retirement announcements, job announcements, pistol meets, holiday cheer messages, and CLETS inquiries that are for personal use.

   2. Profane or obscene language for any purpose including that contained within the description of a crime.

3. Excessive listing or detailed description of stolen property except that identifiable by serial numbers or unique markings.

4. Subpoenas relative to civil proceedings, or any subpoenas which could be delivered in a timely manner by other means. All subpoenas transmitted via CLETS must be processed in accordance with Sections 1328 b and 1328 c of the California Penal Code.

5. Lost identification cards/badges, other than those listed in A.7. (When possible, this information should be entered into the Automated Property System.)

1.6.6 Local/Wide Area Networks - Definition and Requirements

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

A. A LAN/WAN system upgrade application and diagram shall be submitted to the CLETS Executive Secretary for review by the CLETS Advisory Committee. The application package shall include standards, protocols, operating systems, servers, the type of security and how it is being used, and Internet Protocol (IP) and Media Access Control (MAC) addresses.

B. Each LAN/WAN work station and/or communication server shall have a fixed address permanently assigned as a CLETS mnemonic. No random selection or pooling of 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-ten alpha-numeric character supplemental header plus the extended headers with the Operator Identification Field (OIF) (see Section 1.6.7) and a Terminal Address Field (TAF), if used (see Section 1.6.8).

   1. LANs using Transmission Control Protocol/Internet Protocol (TCP/IP) should transmit the IP and Media Access Control (MAC) addresses, if available, in the TAF.

   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 CLETS information. This prohibition does not apply to:

1. Terminals used for remote vendor access.

2. Terminals used to access CLETS on behalf public law enforcement/criminal justice agencies by the following public entities: communication centers, law enforcement/criminal justice consortiums, and agencies performing parking enforcement. (See Section 1.5 for appropriate contractual agreements.)

E. In an untrusted network, those segments which will be used to transport CLETS data must either:

1. Be segmented from the untrusted portion of the network by a firewall. The firewall shall be controlled by the law enforcement/criminal justice agency or their designee. A minimum firewall profile must be implemented to provide a point of defense, control, and audit access to CLETS data as referenced in Section 1.9.4. Information on minimum firewall profiles can be found at the following websites: www.certicom.com and www.trusecure.com OR

2. Be encrypted while in the untrusted network segment. It is incumbent upon the agency to ensure on a regular basis that their encryption method meets the minimum-security standards as specified in the CLETS Technical Guide.

Agencies initiating use of a public network must comply at the time of implementation with the minimum-security standards as specified in the CLETS Technical Guide. Agencies already approved for utilizing a public network to access CLETS on that date must be in compliance with these standards prior to June 2008.

1.6.7 Operator Identification Field Requirements

All Message Switching Computers (MSC), Computer Aided Dispatch (CAD) systems, and Local/Wide Area Network (LAN/WAN) systems must transmit a unique User-ID as an extension of the four-to-ten alpha-numeric character supplemental header. The Operator Identification Field (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 CLETS information shall be uniquely identified with a User-ID and password. The User-ID can take the form of a name, badge number, serial number, or other unique number.

B. Each terminal operator must log on with a 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 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 CLETS in the Operator Identification Field (OIF).

D. 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.

Refer to the *CLETS Computer Interface Rules and Requirements* for complete message header and format information.

1.6.8 Terminal Address Field Requirements

All Message Switching Computers (MSC), Computer Aided Dispatch (CAD) systems, and Local/Wide Area Network (LAN/WAN) systems should transmit a Terminal Address Field (TAF). The TAF is a 6 to18 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 Transmission Control Protocol/Internet Protocol (TCP/IP) can transmit the IP and Media Access Control (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.

Refer to the *CLETS Computer Interface Rules and Requirements* for complete message header and format information.

1.6.9 Dial-up/Wireless Access to CLETS

CLETS information is normally transmitted via private, dedicated lines. However, access to CLETS may be achieved on a public switched line using a dial-up/wireless system upon approval by the CLETS Advisory Committee. Dial-up/wireless access is allowed from a terminal through its host server or message switching computer (MSC) system. Access to CLETS via the Internet is not allowed.

An application for dial-up/wireless access must be submitted through the CLETS Executive Secretary to the CLETS Advisory Committee for approval. The form and content of the application will be prescribed by the Department of Justice. All information and requests should be directed to the address listed in Section 1.1.4.

The subscriber 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 comments will be addressed to the CLETS Advisory Committee through its CLETS Executive Secretary. The CLETS Executive Secretary will review and submit the completed application to the CLETS Advisory Committee for approval. Changes to the application should be in writing.

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 Department of Justice, CLETS Administration Section. Mnemonics assigned for such purposes must be used only on terminals designated for dial-up/wireless access. CLETS mnemonics shall not be assigned to vendor terminals.

    3. All logons, successful and unsuccessful, must be logged. Repeated failed log on attempts shall disable the user account. Such logs must be retained by the agency for three years.

    4. Personnel leaving the agency for any reason or no longer authorized access to CLETS must have their User-ID and password deleted by the local agency and host MSC administrator immediately.

B. All CLETS information 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 CLETS by utilizing a ciphered User-ID and password security to access the communications. It is

incumbent upon the agency to ensure on a regular basis, that their encryption method meets the minimum-security standards as specified in the CLETS Technical Guide.

2. Agencies initiating use of a dial-up/wireless system that traverses a public network must comply at the time of implementation with the minimum-security standards as specified in the CLETS Technical Guide. Agencies already approved for utilizing a public network to access CLETS on that date must be in compliance with these standards prior to June 2008.

1.7 SYSTEM DESIGN AND ENHANCEMENT STANDARDS

1.7.1 Message Switching Computer (MSC) Definition and Requirements

A message switching computer (MSC) is that portion of the hardware and software solely designed to pass through transactions to and from CLETS. MSCs shall be maintained with a 98% availability and up-time measured over a continuous twelve month period, including all (scheduled and unscheduled) downtime.

A. All direct interface MSCs shall record all transactions to and from 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 unique operator (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 which also identify the requester and secondary recipient shall meet criminal history 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 message switching computers interfaced with CLETS must follow the *CLETS Computer Interface Rules and Requirements (R&Rs)* adopted by the CLETS Advisory Committee covering such interfaces. Copies of the R&Rs may be obtained from the CLETS Executive Secretary via the Publications Request Form contained in the *CLETS Operating Manual*, Chapter 2. Agencies requesting the R&Rs must note if a system upgrade is pending.

1.7.2 Message Switching Computer Design

Engineering shall be of the design and performance standards acceptable to the CLETS Advisory Committee. Engineering shall include circuitry, terminal equipment, switching devices and interfacing equipment that comprise the makeup of CLETS. Any changes, additions or deletions must be submitted in writing, accompanied by supporting data to justify said request, to the CLETS Executive Secretary for review.

All MSCs planning to relocate must formally advise the CLETS Executive Secretary at least 60 days in advance of the move with the new address, planned move/implementation date, and if test lines and terminal mnemonics are required.

1.7.3 System Upgrade

An upgrade consists of any installation, replacement, or planned enhancement of a directly or indirectly connected host server by a CLETS subscriber agency for purposes of CLETS transactions.

A. The CLETS subscriber agency should inform the host message switch and the CLETS Executive Secretary of an impending upgrade 6 to 12 months prior to projected implementation. The subscriber agency shall submit an upgrade service application to the CLETS Executive Secretary not less than 180 calendar days before implementation. The subscriber agency should direct all information and requests to the address listed in Section 1.1.4.

   The subscriber agency shall forward the completed upgrade application to the County Control Agency/Direct Interface System Host for review and recommendation (see Section 1.4.1). The County Control Agency/Direct Interface System Host comments will be addressed to the CLETS Advisory Committee through its CLETS Executive Secretary. The CLETS Executive Secretary will review and submit the completed upgrade application to the CLETS Advisory Committee for approval. Changes to the application should be in writing.

   Should any request for a subscriber agency's specific engineering change, addition or deletion increase CLETS cost or depart from established CLETS policies or practices, the CLETS Advisory Committee shall have the final decision.

B. A one page network configuration diagram is required with all upgrade applications, and must include the following:

   - agency name, county, and date
   - how the system interfaces with CLETS
   - number, speed and types of data lines
   - hardware and software vendors
   - communications equipment vendor
   - number and vendor name of both fixed and mobile
   - terminals and how they connect to host server
   - remote vendor access, if applicable

C. An upgrade application submitted by a County Control Agency must include an MSC/Users Costs and Requirements form **(reference Exhibit H)**. The County Control Agency must certify that each of the CLETS subscribers behind their interface are 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 Message Switching Computer 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 CLETS Advisory Committee, the agency must request a test line and any test mnemonics in writing from the CLETS Executive Secretary. During the testing period of a new or upgraded system, the agency is responsible for the line, equipment (CSUs/DSUs, modems, line drivers, etc), and installation costs. Testing of upgraded equipment shall not exceed one year unless by written consent of the CLETS Executive Secretary.

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

1.8 TRAINING

1.8.1 Equipment Training

It is the responsibility of the equipment vendor to provide training on the operation of the terminals they supply.

1.8.2 System Training

Agencies with host systems are responsible for training its local users on how to access the MSC and the use of pre-formatted screens.

1.8.3 Database Training

Training in message formats for access to information in the Criminal Justice Information System (CJIS) databases, National Crime Information Center (NCIC), National Law Enforcement Telecommunications System (NLETS), Department of Motor Vehicles (DMV), and Oregon Law Enforcement Data System (LEDS) is the responsibility of the Department of Justice. Training will be accomplished according to the following:

A. It is the responsibility of all city, county, state, and federal agencies that use information supplied via CLETS to participate in the Department of Justice's training programs to ensure that all personnel (i.e. terminal operators, peace officers, investigators, clerical, agency management/supervisors, etc.) are trained in the operation, policies, and procedures of each file that is accessed or updated. Training shall be provided only by the Department of Justice's Field Operations Program 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) in order to ensure compliance with CLETS/NCIC policies and regulations. This is accomplished by completing the required training and the appropriate CLETS/NCIC Telecommunications Workbook published by the Department of Justice, or a facsimile thereof. An agency wishing to make additions or modifications to the Workbook must receive prior approval from the Department of Justice, Field Operations Program.

   2. Biennially, provide functional retesting, and reaffirm the proficiency of all terminal (equipment) operators (full access/less than full access) in order to ensure compliance with CLETS/NCIC policies and regulations. This is accomplished by the completion of the appropriate CLETS/NCIC

Telecommunications Proficiency Examination published by the Department of Justice, or a facsimile thereof. An agency wishing to make additions or modifications to the Examination must receive prior approval from the Department of Justice, Field Operations Program.

3. Maintain records of all training, testing, and proficiency affirmation. An individual computerized or written log must be maintained on each full access operator. Such logs may be destroyed 3 years after the operator is separated from the agency. Training records for less than full access operators, practitioners, administrators, and other sworn/non-sworn law enforcement personnel shall be maintained on a computerized or written group log. Less than full access operator group logs shall be retained indefinitely by the agency. The workbooks and exams may be discarded upon entry of the required information in the appropriate log

4. Initially (within 6 months of employment or assignment) all sworn/non-sworn practitioner personnel must receive basic training in CLETS/NCIC policy and regulations.

5. Make available appropriate training on 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 CLETS/NCIC systems, using methods such as roll call and in-service training.

7. Provide peer-level training on CLETS/NCIC system use, regulations, policies, audits, sanctions, and related civil liability for criminal justice administrators and upper-level managers.

B. To ensure compliance with this training mandate, the Department of Justice is responsible for monitoring the on-going training provided to law enforcement personnel. On-site visits, including classroom observation and review of training records, will be conducted by Department of Justice staff.

1.9 SECURITY

Statewide operational control and system supervision shall be under the direction of the Department of Justice. Monitoring of traffic for conformity to rules and regulations and recommendations for corrective actions shall be the responsibility of said personnel. CLETS access is permitted only from an agency approved device. The CLETS system cannot be accessed through a personally-owned device. Vendors may remotely access CLETS for testing and diagnostic purposes only. Allowing software testing or diagnostics from remote terminals will be at the discretion of the agency head.

Each system interfacing CLETS shall assist the Department of Justice in overseeing new and upgrade application hardware, software, and security of the terminals connected to the computer system for compliance to CLETS policies.

In order to maintain the integrity of 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

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 CLETS-provided information 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 notify the CLETS Executive Secretary of the terminal mnemonic and originating agency identifier (ORI) whenever a terminal is suspected of being stolen or misplaced.

1.9.2 Background and Fingerprint Requirements

A. All persons, including non-criminal justice, volunteer personnel, and private vendor technical or maintenance personnel, with physical access to CLETS provided information or to Criminal Offender Record Information (CORI) are required to undergo a background and fingerprint check.

   1. The California Code of Regulations, Title 11, Division 1, Chapter 7, Article 1, requires the following:

      a. Subsection 703(d) states: Record checks shall be conducted on all personnel hired after July 1, 1975, who have access to criminal offender record information.

b. Subsection 707(b) states: Record checks shall be conducted on all personnel hired after July 1, 1975, who have access to the computer system, its terminals, or the stored criminal offender record information.

2. Where CLETS access is available without CORI, all persons, including non-criminal justice and private vendor technical or maintenance personnel, accessing areas where CLETS or CLETS information is located are required to undergo a background and fingerprint check.

3. If the background/fingerprint check reveals a felony conviction of any kind, CLETS 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 criminal justice agency head, or his/her designee, will review the matter and decide if CLETS access is appropriate.

4. Visitors to a computer center, such as a tour group, where the computer center has CORI access are not required to undergo a background and fingerprint check. They must, however, be escorted at all times.

5. 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 CLETS may be sworn law enforcement personnel, non-sworn law enforcement personnel, or non-criminal justice, volunteer personnel, and private vendor technical or maintenance personnel that have been subjected to a character or security clearance to include the following checks:

1. Department of Justice - Bureau of Criminal Identification and Information (BCII) fingerprint check.

   NOTE: <u>All</u> federal agencies are exempt from conducting a Department of Justice fingerprint clearance.

2. FBI fingerprint check

   NOTE: Public agency employees temporarily assigned to a law enforcement or criminal justice agency are not required to obtain fingerprint clearance from the FBI. However, Department of Justice fingerprint clearance <u>is</u> required.

3. Depending on circumstances, other checks may be made to arrive at satisfactory conclusions:

- Employer(s) for the last year
- Local credit association
- High school or other educational institution
- All police files in jurisdiction(s) where applicant has lived
- References
- Any or all previous employers
- Present neighbors
- Military records, if applicable

4. Department of Justice CJIS databases may be accessed, with the exception of the Automated Criminal History and Mental Health Firearms Prohibition Systems, for background investigations of criminal justice employees. This does not preclude the submission of fingerprint cards for a positive means of identification.

C. Personnel shall not operate or have access to CLETS terminals, equipment or information until a background and fingerprint check 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 CLETS access following the completed background and fingerprint check 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 statement form prior to operating or having access to CLETS terminals, equipment, or information. It is recommended that each employee/volunteer sign an employee 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 logins, successful and unsuccessful must be logged. Repeated failed log on attempts shall disable the user account. Such logs must be retained by the agency for three years.

C. When a person with access to CLETS is no longer employed or no longer accessing CLETS on behalf of the law enforcement 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 CA DOJ 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 meeting the FBI's CJIS Security Policy section 7.3.1 shall be used.

2. The VPN encryption method meets the encryption requirements as stated in the FBI's CJIS Security Policy section 7.8.

3. Two factor authentication shall be used where at least one factor must meets the Advanced Authentication standards identified in the FBI's CJIS Security Policy section 7.3.

4. The VPN equipment resides behind a network firewall that meets the requirements stated in the FBI's CJIS Security Policy section 7.10.

5. Terminals with the CLETS access shall employ, at a minimum, a personal/software based firewall. Personal firewalls shall meet the requirements stated in the FBI's CJIS Security Policy section 7.10.2.

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 network firewall that meets the requirements specified in the FBI's CJIS Security Policy section 7.10.

1.10 SYSTEM DISCIPLINE/APPEAL PROCESS

The CLETS Advisory Committee is responsible for overseeing system discipline. Messages/transactions processed through the CLETS network shall be subject to random sampling by the CLETS Advisory Committee, or its designee(s), for validity of content and conformity with the CLETS rules, regulations, policies, practices, and procedures.

1.10.1 System Misuse

A. Violation of CLETS rules, regulations, or policies, practices, and procedures shall be investigated by the CLETS Executive Secretary. Allegations of misuse will be handled as follows:

1. A written report will be provided to the involved agency.

2. A written explanation and statement of corrective action shall be submitted to the CLETS Executive Secretary by the agency head.

3. If the reported explanation and corrective actions resolve the problem, the investigation and results will be reported to the CLETS Advisory Committee by the CLETS Executive Secretary.

4. If the reported explanation and corrective actions do not resolve the problem to the satisfaction of the CLETS Executive Secretary, the head of the agency may be requested to appear before the CLETS Advisory Committee to explain the incident.

5. Unresolved incidents shall be presented to the CLETS Advisory Committee by the CLETS Executive Secretary with a recommendation. The CLETS Advisory Committee will decide on a course of action or sanction to apply. The CLETS Executive Secretary will issue a letter formally notifying the agency of the decision.

B. A violation of law (government or penal code) or CLETS rules, regulations, or policies, practices, and procedures may result in any of the following sanctions, dependent upon the total circumstances of the incident:

1. Letter of censure,

2. Suspension of service - This may be for varying lengths of time and/or may include suspension for specified database or other system services; and/or

3. Removal of CLETS service.

C. Incidents or events brought to the CLETS Advisory Committee under the conditions of Sections 1.10.1.A. 1-4 shall be brought to the attention of the agency head as soon as practical.

1. In the event a hearing is scheduled under the provisions of Section 1.10.1.A.5, 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.

2. If a sanction is imposed by the CLETS Advisory Committee, the effective date of the action shall be ten working days. The ten day notice can be waived if extraordinary circumstances exist.

3. 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 CLETS Executive Secretary on the number of investigations performed related to 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 CLETS Service

The California Department of Justice or the subscriber may, upon 30 days written notice, discontinue service.

State of California
Department of Justice
Attn: CLETS Executive Secretary
P.O. Box 903387
Sacramento, CA 94203-3870

ORI #_____

County_____

CALIFORNIA LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM SUBSCRIBER AGREEMENT

In accordance with Section 15165 of the Government Code, it is hereby agreed that

_____

(Name of Agency or Organization)

hereinafter referred to as Subscriber, as a Subscriber to the California Law Enforcement Telecommunications System (CLETS), will conform to the operating policies, practices and procedures approved by the CLETS Advisory Committee.

It is further agreed by the Subscriber that, in order to receive such criminal history information as is available in the FBI/NCIC files and in the California Department of Justice files, the Subscriber agrees to abide by all rules, policies and procedures of the FBI/NCICI as approved by the NCIC Advisory Policy Board. The Subscriber also agrees to adhere to all rules, policies, and procedures of the National Law Enforcement Telecommunications System (NLETS). No private entity shall be authorized to access CLETS, nor shall CLETS be used on behalf of a private entity for purposes of parking citation enforcement.

It is understood by the Subscriber that violation of these rules, policies, practices, and procedures approved by the CLETS Advisory Committee, the FBI/NCIC Advisory Policy Board, and/or the NLETS Advisory Board may result in suspension of service or other appropriate disciplinary actions as determined by the CLETS Advisory Committee.

The CLETS Advisory Committee reserves the right to immediately suspend furnishing criminal history data to the Subscriber when either security or dissemination requirements approved by the CLETS Advisory Committee are violated.

It is understood by the Subscriber that it is the responsibility of all city, county, state, and federal agencies that use information supplied via CLETS to participate in DOJ's training programs to ensure that all personnel (i.e. terminal operators, peace officers, investigators, clerical, agency management/supervisors, etc.) are trained in the operation, policies, and procedures of each file that is accessed or updated. Subscriber understands that training shall be provided only by DOJ's training staff or another certified CJIS/NCIC trainer. Periodic unannounced site inspections may be performed by the Department of Justice to ensure compliance CLETS rules, regulations, policies, practices, and procedures.

(continued)

Agency Name:_____ ORI # :_____

It is further agreed by the Subscriber that the following training requirements will be followed:

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) by the completion of a workbook (or facsimile thereof) in order to ensure compliance with CLETS/NCIC policies and regulations.

2. Biennially, provide functional retesting, and reaffirm the proficiency of all terminal (equipment) operators (full access/less than full access) by the completion of a proficiency exam (or facsimile thereof) in order to ensure compliance with the CLETS/NCIC policies and regulations.

3. Maintain records of all training, testing, and proficiency affirmation. An individual computerized or written log must be maintained on each full access operator. Such logs may be destroyed 3 years after the operator is separated from the agency. Training records for less than full access operators, practitioners, administrators, and other sworn/non-sworn law enforcement personnel shall be maintained on a computerized or written group log. Less than full access operator group logs shall be retained indefinitely by the agency. The workbooks and exams may be discarded upon entry of the required information in the appropriate log.

4. Initially (within 6 months of employment or assignment) all sworn law enforcement personnel must receive basic training in CLETS/NCIC policy and regulations.

5. Make available appropriate training on 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 CLETS/NCIC systems, using methods such as roll call and in-service training.

7. Provide peer-level training on CLETS/NCIC system use, regulations, policies, audits, sanctions, and related civil liability for criminal justice administrators and upper-level managers.

Either the California Department of Justice or the Subscriber may, upon 30 days notice in writing, discontinue service. This Subscriber Agreement is renewable every three years, when the agency head changes, or immediately upon request of the CLETS Executive Secretary.

_____ _____
Agency Head - Type or Print Title -Type or Print

_____ _____
Agency Head Signature Date

Rev. 8/01

CHANGE REQUEST

Department of Justice
CLETS Administration Section
P.O. Box 903387
Sacramento, CA 94203-3870

Telephone: (916) 227-3677
FAX: (916) 227-0696

_____ _____
Agency Name ORI Number

_____
Agency Address

_____ _____ _____
City ZIP Code County

_____ (____)_____
Name and Title of Person Requesting Change Telephone Number

COMPLETE AREAS REQUIRING CHANGE

Agency Address/Telephone Number Change (see above) ___Yes ___No

Agency Head: _____ (____)_____
Name Telephone

(If new person, complete a new Subscriber Agreement) _____ (____)_____
Address Fax

_____
E-mail Address

Agency Terminal Coordinator (ATC):

_____ (____)_____
Name Telephone

_____ (____)_____
Address Fax

_____
E-mail Address

Security Point Of Contact (SPOC):

_____ (____)_____
Name Telephone

_____ (____)_____
Address Fax

_____
E-mail Address

NCIC/ORION Information (____)_____ (____)_____
Telephone Alternate Telephone

(____)_____ (____)_____
Fax Alternate Fax

Hit Confirmation Please use the separate Hit Confirmation Data form for providing hit confirmation information changes

Signature of ATC or Agency Head: _____ Rev. 09/05

AGENCY TERMINAL COORDINATOR (ATC)
RESPONSIBILITIES

An Agency Terminal Coordinator (ATC) is the key person chosen by his/her respective agency to serve as the coordinator with the Department of Justice (DOJ) on matters pertaining to the use of CLETS, NCIC, NLETS, and the DOJ criminal justice databases.

The ATC should be familiar with all aspects of CLETS, CJIS, NCIC, and NLETS. The ATC's primary responsibilities include:

Administration/Record Keeping

- Coordinate and/or respond to CLETS-related correspondence
- Notify DOJ of changes in address, phone number, agency representatives, and other information pertaining to your agency
- Report to the CAS the number of CLETS misuse investigations conducted by your agency or MSC on a yearly basis, to include type of misuse and outcome
- On a quarterly basis, ensure the accuracy of CLETS user security files within your agency or MSC, deleting users who are no longer employed
- Ensure the recommended Employee Statement forms are completed on all employees accessing CLETS information
- Ensure the Third Party Release Log for CORI information released to individuals outside your agency is complete and accurate
- Ensure Management Control or Interagency Agreements are on file, if applicable
- Maintain a copy of all contractual agreements.

Audits/Inspections/Validations

- Ensure compliance with mandated state and federal auditing requirements
- Coordinate CLETS inspections of your agency with the DOJ Field Representative
- Receive CJIS/NCIC validation lists and coordinate the information validation
- Promptly respond to the DOJ annual Agency Representative and ORI validation requests.

Information/Publications

- Oversee the ordering and proper distribution of publications
- Oversee the proper distribution of policy or database change information.

Policy

- Ensure compliance with CLETS, CJIS, NCIC, and NLETS policies and regulations;
- Ensure CLETS terminals, equipment, and messages are secure from unauthorized access.

(continued)

System

- Maintain and have available a current system diagram
- Maintain and have available a list of all CLETS terminal locations within the agency, identifying whether the terminal is fixed, mobile, behind a LAN/WAN, etc.
- Maintain and have available a list of all CLETS terminal mnemonics, whether static or pooled
- Coordinate any terminal access level changes, requests for additional CLETS mnemonics, and applications for upgrading service.

Training

- Advise terminal operators within your agency of formats used on terminals within your agency or county
- Determine the need and coordinate CLETS related training
- Maintain and have available the CLETS/NCIC training records

I have read and understand the responsibilities of a CLETS Agency Terminal Coordinator.

_____ _____

Signature - ATC Date

_____ _____

Signature - Agency Head Date

_____

Name of Agency

PLEASE RETAIN THIS FORM WITH YOUR AGENCY'S RECORDS.

DO NOT SUBMIT TO THE CALIFORNIA DEPARTMENT OF JUSTICE.

Rev. 6/03

MANAGEMENT CONTROL AGREEMENT

Agreement to allow CLETS access by

_____, _____
(Public law enforcement/criminal justice agency) (ORI)

to_____
(Dispatch, parking citation, or data processing public agency)

to perform_____services on their behalf.
(Type of service)

Access to CLETS is authorized to public law enforcement and criminal justice agencies only (hereinafter referred to as the *CLETS subscribing agency*), who may delegate the responsibility of dispatching, parking citation, or data processing/information technology services to a public agency that is neither a law enforcement agency nor a criminal justice agency (hereinafter referred to as the *Non-CJ agency*). The Non-CJ agency may access information obtained via CLETS on behalf of the CLETS subscribing agency in order to accomplish the above-specified services, if such delegation is authorized, pursuant to Executive Order, statute, regulation, or interagency agreement. A signed Management Control Agreement must be received by the CLETS Executive Secretary prior to the subscribing agency permitting the Non-CJ agency access to CLETS. The performance of such delegated services by an otherwise Non-CJ agency does not convert that agency into a public criminal justice agency, nor automatically authorize access to state summary criminal history information. Information obtained via CLETS is confidential and may 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 or criminal charges.

Pursuant to the policies outlined in the *CLETS Policies, Practices, and Procedures (PPP)* and the Federal Bureau of Investigation's *Criminal Justice Information Services Security Policy*, it is agreed that the CLETS subscribing agency will maintain responsibility for security control as it relates to 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 CLETS systems 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, and other components that make up and support a telecommunications network and related CJIS systems 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 computerized message-switching or database systems utilized by the served law enforcement 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.

(Continued) Rev. 11/02

Agency Name:_____ ORI#: _____

Additionally, it is the responsibility of the CLETS subscribing agency to ensure that all Non-CJ agency personnel accessing CLETS information meet the minimum training, certification, and background requirements which 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 CLETS-obtained information. The minimum requirements include, but are not limited to:

1. Initially (within six months of employment or assignment) train, functionally test, and affirm the proficiency of all CLETS computer operators in order to ensure compliance with CLETS/NCIC policies and regulations, if applicable. Biennially, provide retesting, and reaffirm the proficiency of all CLETS operators, if applicable.

2. State and FBI fingerprint-based record checks must be conducted prior to allowing access to CLETS computers, equipment, or information. If the results of the fingerprint-based check reveals a record of any kind, access will not be granted until the CLETS subscribing agency can review the matter to decide if access is appropriate. If a felony conviction of any kind is found, access shall not be granted.

3. Each individual must sign an Employee/Volunteer Statement Form prior to operating or having access to CLETS computers, equipment, or information.

In accordance with CLETS policy, the CLETS subscribing agency has the responsibility and authority to monitor, audit, and enforce the implementation of this agreement by the Non-CJ agency. The Non-CJ agency agrees to cooperate with the CLETS subscribing agency in the implementation of this agreement, and to accomplish the directives for service under the provisions of this agreement. The Management Control Agreement shall be updated at least every three years, when the head of either agency changes, or immediately upon request from the CLETS Executive Secretary.

_____	_____
Signature (CLETS Subscribing Agency)	Signature (Non-CJ Agency)
_____	_____
Print Name and Title	Print Name and Title
_____	_____
Date	Date

PRIVATE CONTRACTOR

MANAGEMENT CONTROL AGREEMENT

Agreement to allow CLETS access by

_____ _____
(Public law enforcement/criminal justice agency) (ORI)

to_____
(Private Contractor)

to perform _____ services on their behalf.
(Type of service)

Access to CLETS is authorized to public law enforcement and criminal justice agencies only (hereinafter referred to as the *CLETS subscribing agency*), who may delegate the responsibility of performing the administration of criminal justice functions; e.g., dispatching functions or data processing/information services, in accordance to Federal Bureau of Investigation's (FBI) Criminal Justice Information Services Security (CJIS) Security Addendum to a private contractor. The private contractor may access systems or networks that access CLETS on behalf of the CLETS subscribing agency in order to accomplish the above-specified service(s). This Agreement must be received by the CLETS Executive Secretary prior to the subscribing agency permitting access to CLETS. The performance of such delegated services does not convert that agency into a public criminal justice agency, nor automatically authorize access to state summary criminal history information. Information obtained via CLETS is confidential and may 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 or criminal charges.

Pursuant to the policies outlined in the *CLETS Policies, Practices, and Procedures (PPP)* and the FBI's CJIS Security Policy, it is agreed that the CLETS subscribing agency will maintain responsibility for security control as it relates to 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 systems 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, and other components that make up and support a telecommunications network and related CJIS systems 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 computerized message-switching or database systems utilized by the served law enforcement 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.

6/05

Agency Name:_____ ORI#:_____

Additionally, it is the responsibility of the CLETS subscribing agency to ensure that all private contractors accessing CLETS information meet the minimum training, certification, and background requirements which 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 CLETS-obtained information. The minimum requirements include, but are not limited to:

1. Prior to allowing CLETS access, train, functionally test, and affirm the proficiency of all CLETS computer operators in order to ensure compliance with CLETS/NCIC policies and regulations, if applicable. Biennially, provide retesting, and reaffirm the proficiency of all CLETS operators, if applicable.

2. State and FBI fingerprint-based record checks must be conducted prior to allowing access to CLETS computers, equipment, or information. If the results of the fingerprint-based check reveals a record of any kind, access will not be granted until the CLETS subscribing agency can review the matter to decide if access is appropriate. If a felony conviction of any kind is found, access shall not be granted.

3. Each individual must sign an Employee/Volunteer Statement Form prior to operating or having access to CLETS computers, equipment, or information.

In accordance with CLETS policy, the CLETS subscribing agency has the responsibility and authority to monitor, audit, and enforce the implementation of this agreement by the private contractor. The private contractor agrees to cooperate with the CLETS subscribing agency in the implementation of this agreement, and to accomplish the directives for service under the provisions of this agreement. The Management Control Agreement shall be updated at least every three years, when the head of either agency changes, or immediately upon request from the CLETS Executive Secretary.

By signing this agreement, the vendor/private contractor certifies that they have read and are familiar with the contents of (1) the CJIS Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; (4) Title 28, Code of Federal Regulations, Part 20; and (5) the CLETS Policies, Practices, and Procedures, and agree to be bound by their provisions. Criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. Access to criminal history record information and related data is therefore limited to the purpose(s) for which the CLETS subscribing agency has entered into the contract. Misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or redisseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. Accessing the system for an appropriate purpose and then using, disseminating or redisseminating the information received for another purpose other than execution of the contract also constitutes misuse. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_____	_____
Signature (CLETS Subscribing Agency)	Signature (private contractor)
_____	_____
Print Name and Title	Print Name and Title
_____	_____
Date	Date

INTERAGENCY AGREEMENT

(This form is used when a CLETS terminal is given to
an agency other than the CLETS subscribing agency.)

This agreement is between the (CLETS Subscribing Agency) _____
and the (Governmental Agency) _____. This agreement pertains to the placement of a CLETS terminal belonging to the CLETS subscribing agency with the above-named agency. A CLETS subscribing agency may not place a terminal with another agency that meets eligibility requirements for CLETS service as a Class I, Class II, or Class III agency per PPP Section 1.3.1. Such an agency must complete an application for new CLETS service.

In accordance to Section 1.5.2 of the *CLETS Policies, Practices, and Procedures* (PPP), and <u>prior to</u> terminal placement, the following must be completed and agreed to by both agencies:

1. A statute, ordinance, or regulation must exist which requires the governmental agency to perform a law enforcement-related function which necessitates access to DOJ/CLETS provided information.

   A. Check one: Statute _____ Ordinance _____ Regulation _____

   B. Specify code or section # _____

   C. Is a copy of the code or section attached, as required? Yes _____ No _____

2. Identify the CLETS mnemonic(s) which will be placed with the governmental agency and the purpose for which the CLETS information is necessary. The purpose identified may determine the database access level which is granted.

   Mnemonic(s):

   _____

   Purpose:

   _____

3. All CLETS rules, regulations, policies, practices and procedures will be adhered to by all parties involved.

4. All persons of the governmental agency having access to DOJ/CLETS provided information must complete the required background check per PPP Section 1.9.2.

5. 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 1.8.3.

(continued) Rev. 11/02

6. A terminal mnemonic address will be assigned to, and associated with, the CLETS subscribing agency's Originating Agency Identifier (ORI) number, and the CLETS subscribing agency will assume full responsibility and liability of all the CLETS activity. The governmental agency will be listed as the secondary location for the terminal.

7. No terminal will be placed with the governmental agency until all conditions of this agreement are met.

8. This agreement is renewable every three years, when the agency head changes, or immediately upon request of the CLETS Executive Secretary.

A signed copy of this interagency agreement and a copy of the applicable statute, ordinance, or regulation of entitlement to receive CLETS provided information must be submitted to:

CLETS Executive Secretary
P.O. Box 903387
Sacramento, CA 94203-3870

It is understood by all parties that the CLETS Executive Secretary reserves the right to overturn approval of this agreement when CLETS policies, procedures, security, or dissemination requirements approved by the CLETS Advisory Committee are violated.

_____	_____
Signature - CLETS Subscriber Agency Head	Signature - Governmental Agency Head
_____	_____
Print Name and Title - CLETS Subscriber Agency Head	Print Name and Title - Governmental Agency Head
_____	_____
Agency Name - CLETS Subscriber Agency	Agency Name - Governmental Agency
_____	_____
Date	Date
_____	
ORI Number	

RELEASE OF CLETS INFORMATION

(This form is used when CLETS provided information is released
to an agency other than a CLETS subscribing agency.)

This agreement is between the (CLETS Subscribing Agency) _____ and the (governmental agency) _____. This agreement pertains to the release of any information data (verbal or written) obtained via CLETS.

The release of CLETS provided information from a CLETS subscribing agency is authorized on a need-to-know, right-to-know basis. In accordance to Section 1.5.3 of *the CLETS Policies, Practices, and Procedures (PPP)*, and prior to the release of CLETS provided information, the following must be completed and agreed to by both agencies.

1. A statute, ordinance or regulation must exist which requires the governmental agency to perform a law enforcement-related function which necessitates access to DOJ/CLETS provided information.

   A. Check one: Statute _____ Ordinance _____ Regulation _____

   B. Specify code or section # _____.

   C. Is a copy of the appropriate section attached, as required? Yes _____ No _____

2. All CLETS rules, regulations, policies, practices, and procedures will be adhered to.

3. All persons having access to DOJ/CLETS provided information must comply with Background and Fingerprint Requirements, PPP Section 1.9.2, which includes a signed Employee/Volunteer Statement Form.

4. All persons having access to DOJ/CLETS provided information must be trained in the operation, policies, and procedures of each file that is released. Training shall be provided only by a certified CLETS/NCIC trainer and must meet all CLETS training requirements per PPP Section 1.8.3.

All subsequent requests for information by an agency with this form on file will be covered.
A signed copy of this release of information form must be submitted to:

CLETS Executive Secretary
P.O. Box 903387
Sacramento, CA 94203-3870

It is understood by all parties that the CLETS Executive Secretary reserves the right to overturn approval of this agreement when CLETS policies, procedures, security, or dissemination requirements approved by the CLETS Advisory Committee are violated. This Agreement is renewable every three years, when the agency head changes, or immediately upon request of the CLETS Executive Secretary.

_____	_____
Signature - CLETS Subscriber Agency Head	Signature - Public Agency
_____	_____
Print Name & Title - CLETS Subscriber Agency Head	Print Name & Title -Public Agency
_____	_____ _____
Date	ORI Date

Rev. 6/05

RECIPROCITY AGREEMENT

Department of Justice
CLETS Administration Section
P.O. Box 903387
Sacramento, CA 94203-3870

Telephone: (916) 227-3677
FAX: (916) 227-0696

Agreement for: _____ enter/update records

_____ hit confirmations and notice of locate
(attach Hit Confirmation Data form)

In entering into this agreement, both agencies agree to conform to all the California CLETS policies. It is understood by all parties that the CLETS Executive Secretary reserves the right to overturn approval of this agreement when CLETS policies, procedures, security, or dissemination requirements approved by the CLETS Advisory Committee are violated.

_____ _____
Agency Forwarding Messages ORI

_____ _____
Agency Receiving Messages ORI

I agree to be responsible for entering/updating records and/or responding to locate and request for confirmation messages on behalf of the forwarding agency noted above.

_____ _____
Receiving Agency Head Name (Type or Print) Title (Type or Print)

_____ _____
Signature Date

I accept that the receiving agency noted above will be acting on our behalf by entering/updating records and/or responding to notices of locate and requests to confirm records entered by my agency. Also, it is my understanding that copies of all reports for records entered will be delivered to the receiving agency.

_____ _____
Forwarding Agency Head Name (Type or Print) Title (Type or Print)

_____ _____
Signature Date

Rev. 11/02

MSC/USERS COSTS AND REQUIREMENTS

Department of Justice
CLETS Administration Section
P.O. Box 903387
Sacramento, CA 94203-3870

Telephone: (916) 227-3677
FAX: (916) 227-0696

_____ COUNTY

Pursuant to directions from the Department of Justice (DOJ) California Law Enforcement Telecommunications System (CLETS), _____County has informed each of the users served through this Message Switching Computer (MSC) of the following costs and/or requirements associated with implementing or upgrading the MSC.

I. Approximate all costs and/or fees to be charged to users served through this new or upgraded MSC (e.g. specific equipment, access costs, etc.):

A. Initial, one-time costs:
   1. Installation charge _____
   2. Lines and equipment _____
   3. Terminal _____
   4. Any other one-time costs _____

B. On-going costs:
   1. Lines and equipment costs _____
   2. Service fees _____
   3. Terminal rental _____
   4. Any other on-going costs _____

II. Specify all requirements for users served through this new or upgraded MSC (e.g., specific equipment, software, etc.):

A. Software specifications _____
B. Hardware specifications _____
C. Line protocols _____
D. Terminal specifications _____
E. Any other requirements _____

As the county control agent, I certify that the information provided herein has been provided to all county users.

_____ _____
Signature - Agency Head Print - Agency Head Name

_____ _____ _____
Agency Head Title Date ORI Number

Rev. 5/01

EMPLOYEE/VOLUNTEER STATEMENT FORM

USE OF CLETS CRIMINAL JUSTICE INFORMATION AND
DEPARTMENT OF MOTOR VEHICLES RECORD INFORMATION

As an employee/volunteer of _____, you may have access to confidential criminal records, Department of Motor Vehicle records, or other criminal justice information, much of which is controlled by statute. All access to California Law Enforcement Telecommunications System (CLETS) related information is based on the "need to know" and the "right to know". Misuse of such information may adversely affect an individual's civil rights, and violates the law and/or CLETS policy.

Penal Code Section 502 prescribes the penalties relating to computer crimes. Penal Code Sections 11105 and 13300 identify who has access to criminal history information and under what circumstances it may be released. Penal Code Sections 11141-11143 and 13302-13304 prescribe penalties for misuse of criminal history information. Government Code Section 6200 prescribes the felony penalties for misuse of public record and CLETS information. California Vehicle Code Section 1808.45 prescribes the penalties relating to misuse of Department of Motor Vehicle record information. Penal Code Sections 11142 and 13303 state:

> "Any person authorized by law to receive a record or information obtained from a record who knowingly furnishes the record or information to a person not authorized by law to receive the record or information is guilty of a misdemeanor."

Any employee/volunteer who is responsible for CLETS misuse is subject to immediate dismissal from employment. Violations of the law may result in criminal and/or civil action.

I HAVE READ THE ABOVE AND UNDERSTAND THE POLICY REGARDING MISUSE OF ALL CLETS ACCESSIBLE INFORMATION.

_____ _____
Signature Print Name

_____
Date

Rev. 6/02

CLETS MISUSE INVESTIGATION REPORTING FORM

Department of Justice
CLETS Administration Section
P.O. Box 903387
Sacramento, CA 94203-3870

Telephone: (916) 227-3677
FAX: (916) 227-0696

Calendar Year _____

(Submit this form by February 1 of each year for the previous calendar year. Include the number of investigations performed related to CLETS misuse, including any disciplinary action taken.)

_____
Agency Name

_____
Address

_____
Person Completing Form

(_____)_____ _____
Telephone Number County

---

1. Total number of investigations performed related to CLETS misuse:

   a. Pending _____ + b. Closed _____ = Total Performed _____
   (1a+1b = 2a +2b+2c)

2. Of the total number of investigations performed, how many originated from:

   a. Private citizen complaints _____
   b. Internal within your Department _____
   c. From another agency _____

3. Misuse violations found from investigations (see #4 below): Total Found _____
   (4a+4b+4c+4d)

4. Total numbers of each type of action taken on misuse violations
   (note only the highest level of action taken in each case):

   a. No action taken: _____

   b. Administrative Action:
      Counsel _____ Reprimand _____ Suspension _____

      Resignation _____ Termination _____ Other _____

   c. Criminal Complaints Filed:
      Infraction _____ Misdemeanor _____ Felony _____

   d. Number of convictions from criminal complaints filed:
      Infraction _____ Misdemeanor _____ Felony _____ Unknown _____

GLOSSARY

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

Administrative Message: a point to point CLETS message (including APBs) sent from a terminal and destined for one or more terminals.

Agency Terminal Coordinator (ATC): the individual designated to be an agency's certified CLETS user trainer and terminal coordinator; acts as liaison between the agency and the Department of Justice, CLETS Administration Section in all CLETS functions.

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

Application: formal qualifying paperwork to be filed with the CLETS Executive Secretary, and approved by the CLETS Advisory Committee, when new or upgraded service is requested.

Automated Firearms System (AFS): the Department of Justice CJIS data file containing information regarding firearms registration and lost, stolen or seized firearms.

Automated Property System (APS): the Department of Justice CJIS data file containing information regarding lost or stolen property.

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

Class I-Law Enforcement Agency: a public agency having statutory power of arrest and whose primary function is that of apprehension and detection. Class I agencies include sheriffs, city police departments, California Highway Patrol, Department of Justice, and the Federal Bureau of Investigation.

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

Class III-Law Enforcement Agency: a sub-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%) is allocated to the administration of criminal justice. Class III agencies include local, state or federal agencies such as: Department of Insurance - Fraud Division; Employment Development Department - Investigations Bureau; military police; and fire department-arson investigations units.

CLETS Administration Section (CAS): the Department of Justice unit that administratively manages the CLETS network; issues terminals and their access authorizations; provides technical consultation services to CLETS clients for planning and implementing both new and upgrading message switching computer (MSC) systems; provides staff support to the CLETS Advisory Committee; and distributes CLETS manuals.

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

CLETS Executive Secretary: provides staff support to the CLETS Advisory Committee and is manager of the CLETS Administration Section; responsible for investigating allegations of CLETS misuse; develops and

enforces all CLETS Advisory Committee approved policies and CLETS security requirements; develops all technical requirements for access to CLETS by computer systems; and oversees the assignment of all CLETS terminal mnemonics and access authorizations.

CLETS Information: any information, or data obtained from any of the databases, when accessed via the California Law Enforcement Telecommunications System (CLETS). This definition does not supercede any statutory or other requirements that apply to the specific data.

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

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

Criminal History System (CHS): the Department of Justice CJIS data file containing compiled records of arrests and court disposition information on subjects.

Criminal Justice Information System (CJIS): the computerized California data files at the Department of Justice, and maintained by local law enforcement agencies and/or the Department of Justice. Data files include: Automated Firearms System (AFS), Automated Property System (APS), Criminal History System (CHS), Domestic Violence Restraining Order System (DVROS), Mental Health Firearms Prohibition System (MHFPS), Missing/Unidentified Persons System (MUPS), Supervised Release File (SRF), Stolen Vehicle System (SVS), Wanted Persons System (WPS), Violent Crime Information Network (VCIN) and Sex and Arson Registration System (SARS).

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

Department of Justice (DOJ): the California state department which maintains and operates the CLETS and CJIS data files; acts as the NCIC and NLETS control terminal agency for California; and performs numerous service functions for law enforcement agencies.

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

Dial-up Access: a method of transporting CLETS messages using public switched telephone lines, and available through special application only.

Direct Access: accessing CLETS with a direct line to the Department of Justice rather than via the county control agency's message switching computer.

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

Domestic Violence Restraining Order System (DVROS): the Department of Justice CJIS data file containing information regarding pending and outstanding active restraining orders.

8A1 terminal: a CLETS terminal (not system) certified by DOJ to function on a direct 8A1 protocol non-computer analog line connection to CLETS at 1200 baud line speed.

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

Interstate Identification Index (III): III is the decentralization of the FBI/National Crime Information Center (NCIC) criminal history subject files. When a III query is received, NCIC responds with the full criminal

record information from non-III participating states, and identifies the III-participating states maintaining criminal history files on the subject. NCIC then automatically forwards the query to the III-participating states with records on the subject, and the individual states must respond back to the original inquirer with the criminal history information from their state. III promotes the inter-state exchange of criminal history information, with each III participant maintaining their own state's criminal history records, rather than the FBI/NCIC.

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

Law Enforcement Data System (LEDS): the State of Oregon's telecommunications system. LEDS maintains a direct interface with California law enforcement agencies, thereby enabling CLETS users to query Oregon's databases, and vice versa.

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

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

Media Access Control (MAC) Address: the hard-wired, port address of a Local Area Network (LAN) based terminal.

Mental Health Firearms Prohibition System (MHFPS): the Department of Justice CJIS database containing information regarding individuals who are prohibited from owning or carrying a firearm due to mental health restraints.

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

Missing/Unidentified Persons System (MUPS): the Department of Justice CJIS database containing information regarding missing and unidentified living or deceased persons.

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

Mobile Data Terminal (MDT): a CLETS terminal with mobile capability, usually located in a patrol car, and includes lap tops, hand held devices, or other transportables.

MSC administrator: the individual responsible for coordinating CLETS-related issues with the Department of Justice.

National Crime Information Center (NCIC): the nationwide computerized data files maintained by the Federal Bureau of Investigation, and composed of data files similar to those in CJIS but at the national level, plus additional files.

National Law Enforcement Telecommunications System (NLETS): the interstate computerized telecommunications backbone system which provides a connection to every state, and allows law enforcement agencies to send/receive information from other states databases and law enforcement agencies.

Network-Public: a common carrier ATM or Frame Relay network where by virtue of their design, the redundancy that is provided, is done so through the use of shared public switches within the network cloud.

Network-Trusted: a network used exclusively by law enforcement/criminal justice agencies and managed by those agencies or their designees as set forth in a Management Control Agreement.

Network-Untrusted: a network that may host a combination of law enforcement/criminal justice agencies and non-criminal justice activities/users.

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

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

Public Network: (see Network-Public)

Static Terminal Mnemonic:. (see Terminal Mnemonic, Static)

Stolen Vehicle System (SVS): the Department of Justice CJIS database containing information regarding lost, stolen, stored, or impounded vehicles, vehicle license plates, or vehicle parts.

Subscriber Agreement: a required agreement for participation in CLETS, and signed by the head of each subscriber agency. The agreement states the subscriber will abide by all rules, requirements, policies, practices, and procedures established by CLETS, CJIS, NCIC, and NLETS.

Supervised Release File (SRF): a CJIS database file of active CDC and CYA parolees, county and federal probationers, sex and arson registrants, violent offenders, and career criminals. The SRF allows law enforcement to send a Contact Message advising the supervising officer of all encounters with the subject.

Supplemental Header: the four-to-ten character field containing alpha/numeric characters generated from a message switching computer with every CLETS transaction and returned with every response. The first four characters of the supplemental header must be the terminal mnemonic which identifies a unique CLETS terminal as the originator of the message; characters five through ten are for use by the MSC.

TCP/IP: Transmission Control Protocol/Internet Protocol; a type of message transmission method used by Local Area Network (LAN) based terminals, and used by the Department of Justice as the primary means of line connection to a direct interface message switching computer.

Terminal: a personal computer, teletype machine, or work station with CLETS access, fixed or mobile.

Terminal Address Field (TAF): the 6 to 18 position fixed/variable length field containing alpha/numeric characters that include a terminal's Internet Protocol (IP) and/or Media Access Control (MAC) addresses. This field is recommended for all terminals accessing CLETS from behind a LAN, and should be transmitted to the CLETS with every transaction.

Terminal Mnemonic: the four character address (terminal name) assigned by the DOJ/CLETS Administration Section (CAS) to identify each CLETS terminal. The terminal mnemonic is transmitted with each CLETS message in the first four characters of the supplemental header. Some non-computer 8A1 terminals remain with three character mnemonics.

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

Time Activated Message Forwarding (TAMF): the CLETS programming feature that allows a specific terminal's messages to be automatically forwarded to another designated terminal on a temporary or continuous basis on specific days and times, e.g., daily from 5:00 p.m. to 7:00 a.m.

Trusted Network: (see Network-Trusted)

Untrusted Network: (see Network-Untrusted)

User ID: the information that determines the identity of a terminal operator and is transmitted in the six-character Operator Identification Field (OIF) with each CLETS transaction.

Volunteer Personnel: agency personnel which may include individuals, such as Reserves, law enforcement Explorer Scouts, law enforcement Cadets, student workers, and senior citizen volunteers.

Wanted Persons System (WPS): the Department of Justice CJIS data file containing information regarding persons with outstanding warrants in California.

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

INDEX
(Subject and corresponding PPP section number)

D

E

F

N

O

P

R

S

T

U

V

W