

## 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.~~

#### 1.1.21 Purpose of the CLETS

~~Pursuant to the GC section 15151, the 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.~~ is an efficient law enforcement communications network available to all public agencies of law enforcement within the state. For interstate access, see section 1.5.5.~~

#### 1.1.32 State Provided Services

~~Pursuant to GC 15161-15163, the CA DOJ shall provide 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 (one location in each county)~~ to handle law enforcement message traffic. Circuitry and terminal equipment to extend beyond, or other than, the CLETS termination point in each county will be provided by client agencies.~~

#### 1.1.43 Request for General Information

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

CLETS ~~Executive Secretary~~ Administration Section  
Department of Justice  
P.O. Box 903387  
Sacramento, CA 94203-3870  
Telephone (916) 227-3677, FAX Facsimile (916) 227-0696  
Email address CAS@doj.ca.gov

## DOJ RATIONALE

- Section 1.1 Purpose and System Description – This section was condensed to reflect what is written in the statutes pertaining to the CLETS.

## FIELD COMMENTS

- The new language does not contain “why” CLETS exists (the purpose) only the “what” CLETS is and “for whom” it is available.
- Language is being deleted that currently states “...The State has an unmistakable responsibility to give full support to all public agencies of law enforcement...”

Instead the replacement states “CLETS is an efficient law enforcement communications network available to all public agencies of law enforcement within the state...”

Why would reference to DOJ supporting the users be removed?

- There is still no purpose stated – it’s in title, but not defined.

## 1.2 **THE CLETS ADVISORY COMMITTEE (CAC)**

### 1.2.1 **Responsibilities of Committee**

The responsibilities of the CLETS Advisory Committee (CAC) are defined in ~~California Government Code Sections~~ GC sections 15154 through ~~15167~~ 15164.

### 1.2.2 **Subcommittees**

The chairperson of the ~~CLETS Advisory Committee~~ CAC 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~~ may be established to evaluate the legislative, user, and technical environment of the CLETS in order to make timely recommendations to the CAC, and perform or update planning functions or documents as directed by the CAC, ~~and to update the CLETS Strategic Plan as needed~~. The following work groups ~~shall~~ may be established under the direction of the SSPS: Administration, Technical, and Legislation.

## **DOJ RATIONALE**

- Section 1.2 The CLETS Advisory Committee (CAC) – The rationale for the change from “shall” to “may” regarding the establishment of a Standing Strategic Planning Subcommittee (SSPS), the Administration, Technical and Legislation Working Groups was to allow members of the SSPS and its working groups the flexibility to participate in and be members of other DOJ committees or working groups.

## **FIELD COMMENTS**

- 1.2.1 / 1.2.1 - Government Code Sections 15165 – 15167 have been eliminated. Section 15165 includes the requirement for submission of Subscriber Agreements and it authorizes suspension of CLETS service for agencies that fail “to conform to the operating policies, practices and procedures approved by the committee...” Will there no longer be an ability to suspend an agency’s CLETS service if misuse occurs? If the ability to suspend service is to continue, who is now authorized to suspend service? This is the ultimate control mechanism for agency compliance and needs to continue.

- 1.2.2 / 1.2.2 - If the SSPS (or the Administration, Technical, or Legislation work groups) were to no longer exist, what would be the forum and process for agencies to provide input and feedback on CLETS user, technical, or legislative issues? Agencies need a voice in the CLETS and I do not envision the CAC wanting to be the first point of involvement.
- Section 1.2.2 Subcommittees: By changing "shall" to "may", I think the structure of the CAC is being compromised. The SSPS and the workgroups beneath it have a vital function within the CAC. The CAC members cannot expect to be fully versed in all matters of CLETS functions, and thereby cannot be expected to make on-the-spot decisions as to Strategic Plans, changes with technology, etc. They depend upon the review of the work groups to recommend the changes. Consider the strategic plan all by itself. The members of CAC would not have had the time to meet as often as the SSPS did to put together the resulting two documents. They depend on the input of others whose day-to-day job includes working with CLETS in one capacity or another.
- 1.2.2. Subcommittees - Changing language that the SSPS and work groups "shall" be established to "MAY" be established would only benefit DOJ, not the user community. It would also mean that there would be no authority that included the user community for issues that affect the user community so greatly (i.e., policy, user access and/or approvals, etc.).

If the above-mentioned changes were made that removed all CAC influence and/or approval authority, then it could be left to the DOJ (not to CAC) if any SSPS or Work Groups ever met again.

Although the DOJ states that they have numerous "user" meetings that could serve the same needs, they are not considered open meetings, have never been advertised, and have been by invitation only (as most in the user community have not heard of them). The DOJ is not required to advertise their business as the CAC is, and this alone could easily result in only those of like mind being invited.

A prime example is how these existing policies were recently brought to CAC at the June 2008 meeting. The policy brought forward did not follow the existing procedures for policy review that have been long practiced, which includes the following:

- Since the development of the work groups, policy was first brought to, or developed at, the Administrative Work Group. Additionally, if the issue was 'technical' the policy would also have been heard by the Technical Work Group. AWG drafted and/or reviewed drafted policy, and then 'voted' to approve and forward the 'proposed' policy to the SSPS.

- SSPS then reviewed, and approved, any and all policy prior to being heard by the CAC. Additionally, not only is the SSPS to hear all policy prior to CAC, but in the August 30, 2001, CAC meeting (found in the CAC minutes), it was decided that SSPS could no longer review any proposed policy the day prior to a CAC meeting (if that policy was going to be heard at the next day's meeting). This shows that SSPS was always expected to review policy changes.

This issue came up because SSPS, in the past, had always met the day before a CAC meeting (assisting in travel for many of the participants). However, many times the SSPS review of the policy resulted in numerous changes that had to be made prior to the policy going forward to CAC. The primary problem with this was that CAC had already received their draft of the proposed policy to review and the policy presented the next day was now contrary to what they had in possession (which already had CAC member comments or other discussion notes).

Not only do the Work Groups and SSPS include "user" feedback, but they ensure the meetings are published and held open, thus allowing for any user participation.

- With budget restrictions, the Business Managers Alliance (BMA) meetings & the CAC meetings should be back to back – not a week or two apart.
- Add the ATCs to the list of BMA participants for notification purpose.

### 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~~ The CAC Meetings

~~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. Pursuant to GC section 1518, the CAC shall meet at least twice each year. Proxies are not allowed for any member who is unable to attend a meeting.~~

## DOJ RATIONALE

- Section 1.2.4 The CAC Meetings – In the current PPPs, this section stated that if a member was unable to attend, they could send an alternate; however, the alternate could not vote. In this version of the PPPs, this section took into account that alternates could not vote and the language was updated to read proxies are not allowed.

## FIELD COMMENTS

- 1.2.4 / 1.2.4 - “Pursuant to GC section 1518” should be “Pursuant to GC section 15158”.
- 1.2.4 - Why has the language allowing CAC members to send an alternate been removed? It still mentions that they substitute cannot vote, but the language referencing sending the alternate is removed.
- Allow proxies to have a vote.

### 1.3 QUALIFICATIONS FOR MEMBERSHIP IN THE CLETS

#### 1.3.1 Eligibility for the CLETS Service

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

- ~~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.~~

## **DOJ RATIONALE**

- 1.3.1 Eligibility for the CLETS Service – The distinction of classes previously listed in the PPPs were deleted and substituted with Law Enforcement Agency for Class I, Criminal Justice Agency for Class II and sub-unit for Class III. These terms are more consistent with the FBI's National Crime Information Center definition. The priority access statement was removed because all of the CLETS users have the same priority.

## **FIELD COMMENTS**

### 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 CA DOJ (see Section 1.1.4.3 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.

Routine applications will be approved by the CA DOJ. Non-routine applications that may result in a policy change, will be brought before the CAC.

### DOJ RATIONALE

- 1.3.2 Applicant Request for Service – To provide better service to client agencies, the requirement for the CAC to approve applications was modified to allow the CA DOJ to approve routine applications for the CLETS. Currently, client agencies may wait for months for approval of their application because the CAC meets only two to three times a year. The CA DOJ should approve all routine applications, whether new or upgrade, rather than require applicants to wait for the CAC approval. However, any application that is not routine, whether new or upgrade, and may result in a policy change, will be brought before the CAC.

The CA DOJ provides a 7 tiered approval process for new applications and a 5 tiered approval process for upgrade applications. For new applications, the tiers include the FBI, the County Control Agency/Direct Interface System Host, an administrative approval from the CA DOJ CLETS Administration Section, a site inspection from the CA DOJ CLETS Training Section, a connectivity approval from the CA DOJ Network Support Group, a security approval from the CA DOJ Network Security Unit and, if applying for a direct connect or mnemonic pooling, an approval from the CA DOJ CJIS/CLETS Mainframe Support Program. For upgrade applications, the tiers are the same as above minus the FBI approval and CA DOJ CLETS Training Section inspection.

## FIELD COMMENTS

- 1.3.2 / 1.3.2 - How, and by whom, will "Routine applications" be defined? Will there be an appeal process in the event the County Control Agency does not agree with CA DOJ that an application should be approved? If so, what will the appeal process be? Will the same definition of "routine" and the same appeal process be in place for contractual agreements?
- Section 1.3.2 - "Routine" and "non-routine" should be defined. Or clarified, as in "all new applications reviewed and approved by the CAC, and all upgrades reviewed just by DOJ". Also, there should be some type of appeal to the CAC process stated in the PPP, if a DOJ decision is questioned.
- Removal of CAC review and approval of applications will create many inconsistencies in this process. Some questions include:
  - What is the definition of routine, and who makes the decision?
  - If all routine are expected to be approved, what happens if they're not?
  - What are the time frames that the applications will be processed, or is there any?
  - What course of action does a user have if they are not in agreement with DOJ's decision, and how long would it take to get to that point?
  - What type of appeal process would there be?
  - Who monitors any problems with the above?

### 1.3.3 Subscriber Agreement

All agencies participating in the CLETS must file a Subscriber Agreement signed by the agency head ~~with the Attorney General through the CLETS Executive Secretary~~ and submitted to the CA DOJ as required by California Government Code Section GC section 15165. A new Subscriber Agreement (**reference see 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~~ CA DOJ.

### DOJ RATIONALE

- 1.3.3 Subscriber Agreement – The requirement to update the Subscriber Agreement every three years is being deleted. By signing the Subscriber Agreement, the agency head has agreed to follow the CLETS/NCIC policies and regulations. Unless the agency head changes, the agreement is still binding.

### FIELD COMMENTS

- Agreement Forms - All of the agreement forms should be consistent in their requirements. A Management Control Agreement must have the exact wording from Exhibit D1. The PCMCA doesn't state this. Private Contractors must abide by and sign the CJIS Security Addendum. I'm assuming no variations to that form? Whereas for the Reciprocity Agreement, an "example" is provided. No definitive statement is made with the Subscriber Agreement. Is this an example or the required language? Are all the forms samples or specific language?
- Allow for dual signatures – such as: agency head/city manager.

### **1.3.4 Agency Terminal Coordinator (also known as the Terminal Agency Coordinator)**

Each CLETS subscribing agency must designate an Agency Terminal Coordinator (ATC).—The ATC is the key person chosen to who serves as the coordinator with the Department of Justice (DOJ) CA DOJ on matters pertaining to the use of the CLETS, the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC), the National Law Enforcement Telecommunications System (NLETS), and the CA DOJ criminal justice databases and administrative network that the CLETS supports accesses. The ATC will be responsible for ensuring compliance with the CA DOJ/FBI policies and regulations including validation requirements, as well as facilitate the exchange of the CLETS administrative information between the CA DOJ and the 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. The ATC's responsibilities shall be designated by CA DOJ on an ATC Responsibilities Form (see Exhibit C). If an agency requests to have other than a permanent, full-time employee as their ATC, the CA DOJ must be notified in writing and will review the request. DOJ must be notified immediately of a Any change in ATC's designation must immediately be provided to the CA DOJ on the Change Request Form (see Exhibit B)(reference Exhibit B, Change Request Form and Exhibit C, ATC Responsibilities Form).

## **DOJ RATIONALE**

- 1.3.4 Agency Terminal Coordinator (ATC) – The ATC section was updated to allow agencies to utilize a part time employee with the approval of the CA DOJ. This should allow agencies greater flexibility in assigning personnel to serve as the ATC.

## **FIELD COMMENTS**

- What happened to the change in the name of the ATC? It was changed in the policy to “Agency CLETS Coordinator” at the November 29, 2005, CAC meeting.
- The ATC has been given the responsibility for “...ensuring compliance with the CA DOJ/FBI policies and regulations including validation requirements...” ATCs do not have the ability to do this; as they can only “assist in ensuring their department is ...” This responsibility is already

listed in the Subscriber Agreement as the agency head's responsibility, which is the appropriate level it should be at.

- 1.3.4 / 1.3.4 - The title "Agency Terminal Coordinator" was to have been retitled "Agency CLETS Coordinator", however, this change was not implemented. "Agency CLETS Coordinator" is a more accurate description of the position. What are the "validation requirements" being added to the Coordinator's responsibilities and will they be defined on the ATC Responsibilities Form? (The Exhibits were not included in the draft for review).
- Section 1.3.4 - The title Agency Terminal Coordinator (ATC) was changed to Agency CLETS Coordinator (ACC) at the November 29, 2005 CAC Meeting, and this should be incorporated in this revision. The rationale for the change still applies today. ACC is a better definition of the position, especially since there are very few "terminals" in existence anymore.
- Section 1.3.4 Agency Terminal Coordinator and Section 1.3.5 Security Points of Contact: I suggest that 1.3.6 be added to state something like: "Although not recommended, the positions of Agency Terminal Coordinator and Security Points of Contact may be held by the same designated person."
- Clarify who will be accepted as an ATC (part time, vendor, etc).
- Add where to find the CJIS Security Policy.
- Don't change the SPOC and ATC communication link.

### 1.3.5 Security Points of Contact

Pursuant to the FBI's Criminal Justice Information Services (CJIS) Security Policy section 3.4, Each CLETS subscribing agency must designate a Security Point of Contact (SPOC). The SPOC is the key person chosen to who serves as the security coordinator with the Department of Justice (DOJ) CA DOJ on security matters pertaining to the use of the CLETS, the NCIC, the NLETS, and the CA DOJ criminal justice databases and administrative network that the CLETS supports accesses. Any information communicated between DOJ and the SPOC will be shared with the agency's ATC.

The SPOC's responsibilities shall be designated by the CA DOJ on a SPOC Responsibilities Form (see **Exhibit J**). If an agency requests other than may be a permanent, full-time employee; vendor; or consultant. as their SPOC responsibilities shall be designated by DOJ, the CA DOJ must be notified in writing and will review the request. DOJ must be notified immediately of a Any change in the SPOC's designation must immediately be provided to the CA DOJ on the Change Request Form (see **Exhibit B**).

### DOJ RATIONALE

- 1.3.5 Security Points of Contact (SPOC) – The SPOC section was updated to allow agencies to utilize a part time employee with the approval of the CA DOJ. This should allow agencies greater flexibility in assigning personnel to serve as the SPOC.

### FIELD COMMENTS

- The language stating: “Any information communicated between DOJ and the SPOC will be share with the agency’s ATC” has been removed. This was a policy addition due to a very “heated” discussion at an SSPS meeting. ATCs took issue to DOJ contacting other individuals without their input or knowledge, and it was agreed that DOJ would not have this contact with the SPOC without ATC involvement.
- 1.3.5 - Why was “Any information communicated between DOJ and the SPOC will be shared with the agency’s ATC.” deleted from this section? The ATC needs to know about technical issues of concern to CA DOJ, and eliminating the sharing of information could be problematic for the ATC, particularly if the SPOC is a part time employee.

- Have a separate website that SPOCs can access if they are not a law enforcement/criminal justice employee. CLEW is not available to them. They need somewhere to get CJIS Security Policy, etc.
- Include vendors or consultants as SPOCs.
- Comment submitted after the 8/20/08 meeting - In the meeting yesterday, DOJ staff agreed that the focus of Sec. 1.3.5, Security Points of Contact (SPOC)- was on IT support staff. That clarification was very helpful. However, it wasn't known by staff, if the DOJ form that depts. use to identify their SPOCs indicate that such staff must complete and pass a state and fingerprint-based record check.

Sec. 1.5.1 seems to cover the issue, but it wouldn't hurt if elsewhere in the PP&Ps that requirement for the SPOC was specified as well.

## **1.4 — CLETS DIRECT INTERFACE RESPONSIBILITIES**

~~GC 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 the 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.~~
- ~~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~~~~

~~CLETS 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.~~
  - ~~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](http://www.certicom.com) and [www.trusecure.com](http://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.~~

## **1.4 THE CLETS INTERFACES**

### **1.4.1 Connections**

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

- A. County Control Agency - GC section 15161 requires that the CA DOJ provide a basic telecommunications network consisting of no more than two switching centers in the state and circuits/equipment to provide service to one location only in each county in the state. This single interface in each county is referred to as the County Control Agency.
- B. Direct Interface Host System – An agency, other than the County Control Agency, opting to host the CLETS service for other subscribing agencies is referred to as the Direct Interface Host System.
- C. Local Agency Direct Interface – An agency opting to interface directly to the CA DOJ for the CLETS, and not hosting other agencies, is referred to as a Local Agency Direct Interface.

### **1.4.2 Requirements for County Control Agency/Direct Interface System Host**

#### A. Role and Responsibilities

The County Control Agency/Direct Interface System Host serves as the CLETS host agency and establishes the requirements for access through their message switching computer (MSC). It is the responsibility of the County Control Agency/Direct Interface Host System to review all new and upgrade applications to ensure compliance from agencies accessing the CLETS behind their respective MSC.

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

1. The type of circuitry and equipment necessary for access and how it can be obtained.
2. The type of services provided from the host MSC, in addition to the CLETS access, such as countywide databases or dispatching.
3. All fees that will be charged for the CLETS service, equipment rental, line costs, and any additional services.

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

B. Mnemonics

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

1. The subscribing agency must submit a completed "Terminal Access Request Form" to the County Control Agency/Direct Interface System Host
2. The MSC administrator for the County Control Agency/Direct Interface System Host will review the request to ensure it can be accommodated by the MSC, sign the request, and forward it to the CA DOJ.

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

C. Network Security

The County Control Agency/Direct Interface System Host is responsible for the integrity and security of the network segment which hosts the CLETS MSC. Pursuant to GC section 15164.1, the County Control Agent or chief officer of any other agency that has been granted direct access to the CLETS shall have sole and exclusive authority to ensure that the equipment of the county or other agency connecting to the CLETS complies with all security requirements as required by the CA DOJ and the FBI.

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

Network segments which host the CLETS message switch/CA 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 or criminal justice agency or their designee. A minimum firewall profile must be implemented to provide a point of defense, control, and audit access to the data accessed via the CLETS as referenced in section 1.9.9.

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

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

### **1.4.3 County Control Agency**

#### **A. Role and Responsibilities**

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

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

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

1. Eligibility for the CLETS service as identified in section 1.3.1 of the CLETS Policies, Practices and Procedures (PPPs).
2. Compliance to the CLETS PPPs and the FBI's CJIS Security Policy.
3. A need for the CLETS service exists to support the normal activities of the applicant and, if facilities such as hardware ports or digital sending units, and the physical computer room space are available at the CLETS point of entry into the county, or adequate technology is available to serve the applicant. If the room capacity is inadequate or essential facilities are unavailable at the time of application, the County Control Agency will have one budget cycle, approximately 18 months, to accommodate the new subscriber.

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

#### B. Upgrade Requirements

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

### 1.4.4 Direct Interface System Host

#### A. Role and Responsibilities

A local agency with a direct interface to the CLETS may provide a CLETS interface to requesting agencies. Agencies wishing to act in

the capacity of a Direct Interface System Host do so at their own expense and through application to the CA DOJ.

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

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

1. Provide written notification, no less than 60 days, to the current County Control Agency advising them of the plans to change to a Direct Interface System Host, including projected dates, if applicable.
2. Forward a completed application to the Direct Interface System Host agency who, in turn, will review the application and accompanying system diagram for the same criteria as defined for the County Control Agency in section 1.4.3.A.

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

#### B. Upgrade Requirements

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

#### C. Termination of Service Requirements

If the Direct Interface System Host wishes to terminate existing service to the subscribing agency, the Direct Interface System Host is

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

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

#### **1.4.5 Local Agency Direct Interface**

##### **A. Roles and Responsibilities**

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

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

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

B. Upgrade Requirements

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

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

A. Local Agency Responsibilities

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

B. County Control Agency Responsibilities

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

1. Recommend approval for immediate access.
2. Recommend approval for access after a specified time frame.

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

C. Inability of the Local Agency to Gain Access through the County Control Agency

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

**1.4.7 Removal of County Control Agency/Direct Interface System Host**

In the event that it becomes evident to the CA DOJ that an existing County Control Agency/Direct Interface System Host cannot fulfill its

responsibilities for any reason or if a County Control Agency fails to provide the CLETS service to qualified applicants or users, it shall be the responsibility of the CA DOJ in consultation with the CAC to seek immediate remedy through coordination with the County Board of Supervisors or the City Council.

## DOJ RATIONALE

- 1.4 The CLETS Interfaces – The entire CLETS Interface section was rewritten to make it easier to understand. The current PPP section 1.4 lists the responsibilities for each of the three interfaces in several sections. The proposed section 1.4 puts the duties of each of the three types of the CLETS interfaces together so it should be easier to understand and follow. Reference to the CAC was deleted from this section since 1.3.2 was reworded to allow the CA DOJ to approve routine new and upgrade applications.

## FIELD COMMENTS

- 1.4.2 / New Section - The proposed order of Section 1.4 does not make it easier to understand. Currently Section 1.4.2 precedes Sections 1.4.3 (County Control Agency) and 1.4.4 (Direct Interface System Host), but it includes roles and responsibilities for both before they are clearly defined. Moving Section 1.4.2 to follow Sections 1.4.3 and 1.4.4 or deleting Section 1.4.2 and incorporating the information contained therein into Sections 1.4.3 and 1.4.4 would help.
- 1.4.2.A / 1.4.1 - How and where is the new responsibility for the County Control Agency/Direct Interface Host System, "...to review all new and upgrade applications to ensure compliance from agencies accessing the CLETS behind their respective MSC." defined? Technical system compliance has been, and needs to remain, the responsibility of CA DOJ. This language needs clarification, as it could be very onerous for County Control Agencies.
- 1.4.1 - Removes language that county controls "shall" provide services to any law enforcement agency that is qualified.
- 1.4.2.B.2 - What is to happen if the MSC cannot accommodate the mnemonic request?
- 1.4.3 - The Sheriff will serve as the county control agency unless the Sheriff's Office indicates another law enforcement agency? What about those few that are not county control now, could they change it?

How can a county control agency possibly ensure all agencies behind them are compliant with all policies? They don't have a staff that could do this, and DOJ currently does this.

- 1.4.6 - The old language said to "...send a written request to the County Control Agency and through the CLETS Executive Secretary to the CLETS Advisory Committee." Now it just says to send it to the County Control Agency. CAC should still be a part of this.

The written request made should be to the CAC, not to DOJ.

The appeal process has been removed from this section. What happens when there are issues? Who will be hearing it? One area states the matter will be referred to the CA DOJ. As this would be a very controversial item, it should be handled as a CAC issue, not a DOJ issue.

- 1.4.7 - Similar to #3 above, the severity of this issue should be handled by the CAC, not by DOJ.
- 1.4.2.C. – define public network and bullet it.
- 1.4.2.C – point back to CJIS Security Policy – when reference is made to a section, state if it's PPP or CJIS Security Policy.
- Define concurrence in 1.4.3.

## 1.5 CONTRACTUAL AGREEMENTS

Any terminal, computer system, or any other equipment that has access to data accessed via the 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~~ CA DOJ.

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

### DOJ RATIONALE

- 1.5 Contractual Agreements – Reference to the CAC was deleted from this section as 1.3.2 was reworded to allow the CA DOJ to approve routine new and upgrade applications. Consistent with section 1.3.2, the CA DOJ will also review and approve routine contractual agreements.

### FIELD COMMENTS

## 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 access to the CLETS equipment or data accessed via the CLETS ~~access~~ 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~~ *CA DOJ* prior to the CLETS subscribing agency permitting the non-CJ agency access to the CLETS equipment or to data accessed via the 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~~ A non-CJ agency may access the CLETS equipment or data accessed via the CLETS 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, ordinance, 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 or the CA DOJ/FBI criminal justice databases.

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

1. Standards for the selection, supervision, and termination of personnel. This does not grant hiring/firing authority to the CLETS subscribing agency, only the authority to grant the CLETS 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 CJS systems CA DOJ/FBI criminal justice databases used to process, store, or transmit criminal justice information, guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.

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

Additionally, it is the responsibility of the CLETS subscribing agency to ensure that all non-CJ agency personnel accessing the CLETS information equipment or data accessed via the CLETS meet the minimum background, training, and certification requirements which that are also imposed on the CLETS subscribing agency's staff. The minimum requirements are applicable also to staff having access to record storage areas containing data accessed via the CLETS-obtained information. The minimum requirements ~~include, but are not limited to:~~ are provided in section 1.9.2.

- ~~1. 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.~~
- ~~2. Each individual must sign an Employee/Volunteer Statement Form prior to operating or having access to CLETS computers, equipment, or information.~~
- ~~3. All persons having access to DOJ/CLETS provided information must be trained in the operation, policies, and procedures of each file that may be accessed or updated. Training shall be provided only by a certified CLETS/NCIC trainer and must meet all CLETS training requirements. per PPP Section 1.8.3.~~

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~~ Data accessed via the CLETS is confidential and may shall be used only for the purpose(s) for which it is authorized. ~~Violation of confidentiality requirements or access authorizations may be subject to disciplinary action, civil action and/or criminal charges.~~

The Management Control Agreement shall be updated ~~at least every three years,~~ when the head of either agency changes, or immediately upon request from the ~~CLETS Executive Secretary~~ CA DOJ.

**Exhibit D1** is a sample agreement ~~which has been approved by the CLETS Advisory Committee and NCIC in regard to its policy~~ that meets the CA DOJ and the FBI requirements. A management control agreement ~~which~~ that is entered into by two or more agencies must incorporate the exact wording of the sample agreement, but may be expanded to meet other requirements of the participating agencies, so long as any expansion is not inconsistent with the language in Exhibit D1.

#### B. Private Contractor

The Private Contractor Management Control Agreement (see Exhibit D2) is required when a CLETS subscribing agency allows access to the CLETS access equipment or access to record storage areas containing data accessed via the 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~~ section 1.5.1.A are applicable for private contractors.

In addition, all private contractors authorized access to the CLETS equipment or data accessed via the CLETS ~~obtained information~~ must abide by and sign the NCIC's FBI's CJIS Security Addendum (see Exhibit K). Vendors with remote access for testing and diagnostic purposes must also enter into a Management Control Agreement specific to their access.

## DOJ RATIONALE

- 1.5.1 Management Control Agreement – Minimum requirements for access to data accessed via the CLETS was deleted and reference made to section 1.9.2 which now lists the requirements.

## FIELD COMMENTS

- 1.5.1.A / 1.5.1.A - Should "...or interagency agreement." be "Interagency Agreement" (i.e., the form) or does it refer to the relationship between the CLETS subscribing agency and a non-CJ agency? If the later, how is the authorization to occur?

Why was the sentence, "Violation of confidentiality requirements or access authorizations may be subject to disciplinary action, civil action and/or criminal charges." deleted? This statement enforces the importance of confidentiality to employees.

- Paragraph talking about Data accessed via the CLETS is confidential and shall be... Why was violation admonishment taken out?
- Difficult for agency to uphold disciplinary action if not in PPP. This needs to be standardized at the state level and in the PPPs for an agency to enforce.
- Leave examples in under 1.5.1.A - third paragraph.

## 1.5.2 Interagency Agreement for Placement of a CLETS Terminal

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

- A. A statute, ordinance, or regulation must exist ~~which~~ that requires the governmental agency to perform a law enforcement-related function ~~which~~ that necessitates access to receiving data accessed via the DOJ/CLETS provided information.
- B. The heads of both agencies must sign an interagency agreement ~~which~~ that states that all the CLETS/NCIC rules, regulations, policies, practices, and procedures policies and regulations will be adhered to by all parties involved (**reference see Exhibit E**).
- C. A copy of the statute, ordinance, or regulation and the signed interagency agreement must be submitted to the ~~CLETS Executive Secretary~~ CA DOJ for review and approval prior to the placement of a CLETS terminal.
- D. A terminal mnemonic address will be assigned to, and associated with, the CLETS subscribing agency's Originating Agency Identifier (ORI), and the CLETS subscribing agency assumes full responsibility and liability for all the CLETS 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 data accessed via the DOJ/CLETS provided information must complete the required ~~background check~~ fingerprint based criminal offender record information search as per Section 1.9.2.
- G. All persons having access to data accessed via the 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 the CLETS/NCIC training requirements per Section 1.8.32.
- H. A CLETS subscribing agency may not place a terminal with another agency that meets eligibility requirements for the 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~~ CA DOJ 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~~ CA DOJ.

## FIELD COMMENTS

### 1.5.3 Release of Data Accessed via the CLETS Information

The release of data accessed via the CLETS provided information or the NCIC from a CLETS subscribing agency is authorized ~~on a need-to-know, right-to-know basis and under the following conditions~~ bound by the FBI's CJIS Security Policy and the California Criminal Record Security Statutes and Regulations. The FBI's policy applies to data accessed via the CLETS.

~~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. If An agency wishing to provide~~ data accessed via the CLETS delivered information to a non-CLETS subscribing agency, ~~must complete a "Release of Data Accessed via the CLETS Information" form (reference see Exhibit F) must be completed. A copy of this Release of Data Accessed via the CLETS form must be submitted to the CA DOJ to review for compliance and retention in the participant's file. The Release of Data Accessed via the CLETS form shall be updated when the head of the agency changes or immediately upon request from the CA DOJ.~~

- ~~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 CA DOJ.~~

~~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.~~

## DOJ RATIONALE

- 1.5.3 Release of Data Accessed via the CLETS – Section A - Both the FBI's CJIS Security Policy, section 6.4 and the Release of CLETS Information form (which will be renamed to Release of Data Accessed via the CLETS form) require the presence of a statute, ordinance or regulation in order for release of the data, therefore, this section was deleted; Sections B 1 – 4 - These sections were deleted because the same information can be found in both PPP section 1.9.2 and on the Release of CLETS Information form.

## FIELD COMMENTS

- Section 1.5.3 - The Release of CLETS Information form. First off, don't change the title to something ridiculously cumbersome. This is not an improvement. Secondly, items B 1, 2, 3 and 4 should remain in this section, as a specific reference point. Changes in the PPP are reviewed and approved by the CAC. Changes to the actual forms, such as Exhibit F, do not get reviewed or approved by the CAC. This is a process that could allow for future changes to the form that are contrary to specific language in the PPP.
- Suggested language for Release of CLETS Information form, "Release of data from CLETS" form.
- Define what data accessed via CLETS is and define secondary dissemination.
- First paragraph, reference specific sections of CJIS Security Policy and CCR stats & regs

#### 1.5.4 Reciprocity Agreement

Any agency ~~which~~ that agrees to perform record entry/update and/or hit confirmation functions on behalf of another agency must enter into a written agreement or a letter of agreement (~~reference~~ see **Exhibit G** for an example of a Reciprocity Agreement). This Reciprocity Agreement The written agreement or letter of agreement must be signed by the head of each agency and a copy must be submitted to the CA DOJ.

~~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~~ written agreement or letter of 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~~ CA DOJ.

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

#### DOJ RATIONALE

- 1.5.4 Reciprocity Agreement – This section was updated to include the acceptance of a letter of agreement signed by both agency heads. This will provide agencies the flexibility in using either a Reciprocity Agreement form or a letter of agreement.

#### FIELD COMMENTS

### 1.5.5 Interstate Access

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

An Interstate Access Agreement must be completed and submitted to the ~~CLETS Executive Secretary~~ CA DOJ to review for compliance and retention in the CLETS subscribing agency's file. The Agreement shall be signed by the head of the adjacent state system agency and the ~~California Attorney General or his/her designee~~ CA DOJ.

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~~ CA DOJ.

### FIELD COMMENTS

## 1.6 SYSTEM RULES

System rules are designed to provide the most efficient operating system consistent with the needs of law enforcement. Adherence to the rules will ensure client agencies the maximum effectiveness of the CLETS. Violations of the CLETS or NCIC rules will result in an investigation and appropriate disciplinary action as determined by the ~~CLETS Advisory Committee~~. CA DOJ.

### DOJ RATIONALE

- 1.6 System Rules – The reference to the CAC performing an investigation and determining appropriate disciplinary action for violations of system rules was changed to the CA DOJ performing these functions which are consistent with current practices.

### FIELD COMMENTS

- 1.6 / 1.6 - Why was the word “disciplinary” deleted? It is included in the Rationale for the changes in this section. Section 1.6.4.C discusses “...administrative action and/or criminal prosecution.” and a deterrent to CLETS misuse/non-compliance in the introduction to this section is important.
- Not consistent with GC 15154. This is the CAC’s responsibility.

### 1.6.1 Database Policies and Regulations

All users shall abide by all policies and regulations pertaining to the data obtained from databases accessed through via the CLETS. Procedures and message formats contained in user manuals must be followed exactly.

- A. Users must confirm the validity of the positive response on the record by contacting the entering agency prior to taking enforcement actions based solely on that record.
- B. Periodic driver license checks may be conducted on the CLETS subscribing agency employees where driving is a requirement of their job.

~~**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. Details of state summary criminal history information may be received by an agency approved wireless device, provided all wireless access security requirements are met (see section 1.6.9)

D. Pursuant to the California Code of Regulations, Title 11, Division 1, Chapter 7, Article 1, section 707(c), every agency is required to keep a record of each release of criminal offender record information for a minimum of three years from the date of release. Detailed information regarding retention of information can be found in this code section.

GE. The CA DOJ Automated Criminal History System Prohibitions:

1. In reference to U.S. Code, Title 18, Section 922(G)(9), terminals are prohibited from accessing the CA DOJ Automated Criminal History System to enforce the provisions of Title 18 USC section 922(G)(9) which effects 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 (GORI)~~ the CA DOJ Automated Criminal History System through the CLETS for licensing, certification, or employment purposes, including pre-employment background investigations for sworn peace officers and/or law enforcement employees as specified in 830 of the

Penal Code (PC) et al; or for remotely accessing a record for review and/or challenge by the subject of a record.

Exceptions:

- a. ~~Per Pursuant to Education Code Sections ~~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 specific state summary criminal history information accessed via the CLETS on a prospective non-certificated employee or non-teaching volunteer aide. If the law enforcement agency agrees to provide the automated record check state summary criminal history information, the results shall be returned to the requesting district or county office of education within 72 hours of the written request. The law enforcement agency may charge a fee to the requesting agency not to exceed the actual expense to the law enforcement agency. For purposes of this section only, a school police department may not act as its own law enforcement agency.~~
- b. ~~Per Pursuant to Vehicle Code, ~~Section~~ section 2431, the California Highway Patrol (CHP) may utilize the CLETS to conduct preliminary criminal history checks offender record information search on applicants for tow truck driver and owner/driver certificates employers.~~
- c. ~~Section Pursuant to PC section 11105.03, of the Penal Code **allows** a law enforcement agency is authorized to furnish specific state summary criminal history information accessed via the CLETS to a regional, county, city, or other local public housing authority for screening prospective participants as well as potential and current staff. The only state summary criminal history information ~~which~~ that 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. Information released to the local public housing authority shall also be released to parole or probation officers at the same time, if applicable.~~ For purposes of this section only, a housing authority police department may not act as its own law enforcement agency unless approved on an individual basis by the CLETS Advisory Committee CA DOJ.~~

- d. ~~Per the~~Pursuant to the Code of Civil Procedures, ~~Section~~ section 1279.5(e), the courts shall use the CLETS to determine whether ~~or not~~ an applicant for a name change is under the jurisdiction of the Department of Corrections and Rehabilitation or is required to register as a sex offender pursuant to ~~Section~~ PC section 290 of the California Penal Code. If a court is not equipped with the CLETS, the clerk of the court shall contact an appropriate local law enforcement agency ~~which~~ that shall determine whether ~~or not~~ the applicant is under the jurisdiction of the Department of Corrections and Rehabilitation or is required to register as a sex offender pursuant to ~~Section~~ PC section 290 of the Penal Code.
- e. ~~Per Section~~ Pursuant to PC section 11105.6 of the Penal Code, a law enforcement agency may access state summary criminal history information via the 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~~ Welfare and Institutions Code section 16504.5 of the ~~Welfare and Institutions Code~~, county child welfare agency personnel conducting an ~~assessment~~ investigation for the ~~placement of a child~~ purposes described in this code section are entitled to state summary criminal history information ~~obtained through~~ accessed via the CLETS by an appropriate governmental agency. Law enforcement personnel shall cooperate with the requests for the information and shall provide the information to the requesting entity in a timely manner.
- g. ~~CLETS may be accessed to conduct background investigations of candidates for appointment as private, non-professional guardians or conservators.~~ Pursuant to PC section 13202, access to the CA DOJ Automated Criminal History System is allowed for a law enforcement statistical or research purpose only upon approval by the CA DOJ.

~~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.~~

## DOJ RATIONALE

- 1.6.1 Database Regulations – Section B - The reference to Vehicle Code section 1808.45 and home address information remaining in the employee’s personnel file is incorrect and was deleted. The non-disclosure of home address information is generally covered under the need-to know and right know basis under section 1.6.4 Confidentiality of the CLETS Messages. The new sections C & D – This information is being moved up from the old section D which is being deleted. Section E.2.c – This section contains the same information, however, it was just reworded. Section E.2.g - The reference was removed to background investigations of candidates for private non professional guardians or conservators because Probate Code section 2920.5 had a sunset clause of January 1, 2007, and no longer exists. It was replaced with the old section D.4. Old section D 2 and 3 – This information will be moved to the *California Criminal Records Security, Statutes and Regulations* document, which is currently being revised, as these sections deal solely with the use of criminal offender record information.

## FIELD COMMENTS

- Section 1.6.1 - Language that should not be deleted from the PPP are items D 2 and 3 and E and F. These statements are specifically referenced in CLETS training sessions, the CLETS Telecommunications Training for Trainers Guide and Information Bulletins. These items relate to the use and misuse of Criminal History records and are referred to by field reps all of the time. There is no benefit to DOJ or the law enforcement community by having these long standing statements removed. There are plenty of agencies that use these statements in their training, and removing them only confuses the issue of whether these statements no longer apply.
- 1.6.1.E.2 - Why was language removed regarding access of CLETS to conduct background investigations for appointment as private, non-professional guardians or conservators?

Why was language removed on following:

- old 1.6.1.D.2) “Staff of any law enforcement agency or correctional/detention facility may process on-line criminal history inquiries on any visitor to such facility.”?
- (old 1.6.1.D.3) “...records check may be preformed on any person prior to their approval as a ‘ride along’ with...”<sup>6</sup>
- (old 1.6.1.F.) “Test records are available for each database...”
- 830 PC add the word “section” to be consistent throughout the document.
- Tow truck driver and employers – should it be employer not employers?
- Consensus is that old sections D, E & F need to be returned to the document.

## 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~~ the CLETS subscribing sheriffs and police departments must have at least one fixed CLETS terminal with authorization to receive administrative message traffic, unless that agency has an All Points Bulletins Waiver/Release of Liability form on file with the ~~CLETS Executive Secretary~~ CA DOJ. Message traffic for that terminal must directly terminate at a printer ~~and not~~ or to a queue of a terminal staffed 24 hours a day/seven days a week. All fixed CLETS terminals receiving hit confirmation requests or locate messages must directly terminate such messages at a printer ~~and not~~ or to a queue of a terminal staffed 24 hours a day/seven days a week. The CLETS terminal/printer combinations shall have only one mnemonic assigned to the combination, except where a printer may be shared by several terminals.

### B. Mnemonic Pooling

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

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~~ to the CA DOJ for approval. The form and content of the application will be prescribed by the ~~Department of Justice~~. CA DOJ. All information and requests should be directed to the address listed in section 1.1.43.

1. Mnemonic pooling requires the following:

- a. The agency must establish an Access Control Point (ACP) to control the dynamic allocation of mnemonics. The ACP shall provide user authentication and auditing of mnemonics.
- b. The 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. The 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 (TAF), 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~~ ATC and must be available for CLETS ~~the CA DOJ or the FBI~~ inspections. The CA DOJ or the FBI 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~~ that remains inactive for 9 months will be deleted from the CLETS. Inactive mnemonics information will be made available to agencies 90 days prior to deletion.

## DOJ RATIONALE

- 1.6.2.B Mnemonic Pooling – As the CA DOJ currently has an approval process in place for mnemonic pooling, the CAC was removed as the approving body and replaced with the CA DOJ. This is consistent with the changes made in section 1.3.2.

## FIELD COMMENTS

### 1.6.3 Audits and Inspections

Periodic unannounced site inspections and scheduled audits may be performed by the ~~Department of Justice or NCIG~~ CA DOJ or the FBI to ensure compliance with ~~CLETS/NCIG rules,~~ CA DOJ/FBI policies and regulations and 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.

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

### DOJ RATIONALE

- 1.6.3 Audits and Inspections – With the approval of Internet access at the June 25, 2008, CAC meeting, a paragraph is being added in this section to require Internet access records be maintained and made available during audits.

### FIELD COMMENTS

- Explain what will be further inspected.

#### 1.6.4 Confidentiality of the CLETS Messages

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

It is required that each employee/volunteer sign an employee statement form prior to operating or having access to the CLETS terminals, equipment, or information. This form addresses confidentiality, release, and misuse of data accessed via the CLETS information. (see **Exhibit I** for a sample form.)

- A. Data Access to accessed via the 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 data accessed via the CLETS information for non-law enforcement purposes is prohibited, unless otherwise mandated, and is subject to administrative action and/or criminal prosecution.
- D. The CLETS terminals and information data accessed via the CLETS must remain secure from unauthorized access.
- E. Data accessed via the 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 data accessed via the CLETS information retained must be stored in a secure and confidential file.
- G. When an agency determines data accessed via the CLETS information is no longer needed, the information data and/or systems records shall be securely disposed of to prevent access by unauthorized personnel. Such disposal shall include a method sufficient to preclude recognition or reconstruction of information data 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~~ Disposal methods must meet the requirements stated in section 1.9.11.

- H. Information received from a CLETS terminal must be maintained separately from non-law enforcement information.
- I. Terminals must be away from public view with a log on/log off, password process in place.
- J. A unique password must be assigned to each CLETS user and must meet the requirements stated in section 1.9.8.
- 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 section 1.9.6 and 1.9.9 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.

## FIELD COMMENTS

- 1.6.4.K - This is new. Shouldn't it be underlined?

## 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-Administrative Messages, 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.)~~

## **DOJ RATIONALE**

- 1.6.5 Administrative Messages – Sections A & B – These sections were removed as this information is contained in the *CLETS Operating Manual* and should be referenced from that document.

## **FIELD COMMENTS**

### 1.6.6 Local/Wide Area Networks - Definition and Requirements

A Local Area Network (LAN) or a Wide Area Network (WAN) is that portion of the hardware and software that is designed to pass intra-LAN, city/county data, and the CLETS messages direct to the CLETS or through the local ~~Message Switching Computer (MSC)~~. For the 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 the CLETS:

- A. A LAN/WAN system upgrade application and diagram shall be submitted to the ~~CLETS Executive Secretary~~ CA DOJ 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 an auditable address permanently assigned as a CLETS mnemonic. No random selection or pooling of the CLETS mnemonics is allowed unless a mnemonic pooling alternative has been approved for implementation.
- C. All the 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~~ can transmit the Internet Protocol (IP) and Media Access Control (MAC) addresses, if available, in the TAF as referenced in section 1.6.8.B.
  2. All LAN based terminals, regardless of the type of protocol used, should transmit an address equivalent to the MAC. If an IP address is not used or is not available, the MAC address should appear in the first six characters of the TAF. If neither is available, some other uniquely identifying information should be provided.
- D. Non-law enforcement and non-criminal justice agency terminals connected to the LAN/WAN must be prohibited from accessing data accessed via the CLETS information unless authorized by contractual agreements as specified in section 1.5. ~~This prohibition does not apply to:-~~

- ~~1. Terminals used for remote vendor access.~~
  - ~~2. Terminals used to access CLETS on behalf of 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, including all public networks (such as wireless, frame relay, point to point), those segments which that will be used to transport data accessed via the 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 / or criminal justice agency or their designee. A minimum firewall profile must be implemented to provide a point of defense, control, and audit access to data accessed via the CLETS data as referenced in Section 1.9.4.9. ~~Information on minimum firewall profiles can be found at the following websites: [www.certicom.com](http://www.certicom.com) and [www.trusecure.com](http://www.trusecure.com) OR AND~~
  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. Encryption shall meet the minimum requirements as specified in section 1.9.6.~~

~~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.~~

## DOJ RATIONALE

- 1.6.6 Local/Wide Area Networks (LAN/WAN) – Definition and Requirements – Section A - The sentence requiring a LAN/WAN application to be submitted to the CLETS Executive Secretary and reviewed by the CAC was modified to reflect the current approval process in place at the CA DOJ for LAN/WAN applicants as explained in section 1.3.2. Section E – This section was modified to remove reference to the CLETS Technical Guide. All encryption and firewall requirements are now reflected in section 1.9.6 and 1.9.9.

## **FIELD COMMENTS**

- definition of public network – elaborate further.
- point-to-point – what is definition

### 1.6.7 Operator Identification Field (OIF) 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 data accessed via the 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. Passwords must meet the requirements as stated in section 1.9.8.
- B. Each terminal operator must log on with a their own unique User-ID and password, and is accountable for all transactions transmitted under that User-ID and password. The User-ID must be stored by the local MSC/CAD/LAN/WAN or other host server, be available for retrieval and consistent with journal requirements. User-IDs are to be unique to each individual and not reassigned unless there is at least a six-month period between each use.
- C. The local host server will automatically transmit only the User-ID with each message transaction to the CLETS in the ~~Operator Identification Field (OIF)~~.
- D. The CLETS will accept the operator identification information and store the data in the CLETS journal records.
- E. Adequate security controls are required to be maintained over identifiers and passwords.

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

### FIELD COMMENTS

### 1.6.8 Terminal Address Field (TAF) 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 to 18 character variable length field following and separated from the OIF by a period, identified by a number sign, and terminated by a period.

- A. How the TAF is used depends on the method of identification the agency wishes to use.
- B. LANs using ~~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.~~

## FIELD COMMENTS

### 1.6.9 Dial-up/Wireless Access to the CLETS

Data accessed via the CLETS information is normally transmitted via private, dedicated lines. However, access to the CLETS may be achieved on a public switched line using a dial-up/wireless system upon approval by the ~~CLETS Advisory Committee~~ CA DOJ. 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 to the CA DOJ 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~~ CA DOJ. All information and requests should be directed to the address listed in Section 1.1.4 1.1.3.

The subscriber subscribing agency shall forward the completed application to the County Control Agency/Direct Interface System Host for review and recommendation. The County Control Agency/Direct Interface System Host will forward the application and comments ~~will be addressed~~ to the ~~CLETS Advisory Committee~~ CA DOJ through its ~~CLETS Executive Secretary~~ for review. ~~The CLETS Executive Secretary will review and submit the completed application to the CLETS Advisory Committee DOJ 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 CA DOJ. CLETS Administration Section~~. Mnemonics assigned for such purposes must be used only on terminals designated for dial-up/wireless access. The CLETS mnemonics shall not be assigned to vendor terminals.
3. All logons, successful and unsuccessful, must be logged. Repeated failed log on attempts shall disable the user account. All logs must meet the requirements stated in section 1.9.5. ~~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 the CLETS must immediately have their User-ID and password deleted by the local agency and host MSC administrator immediately.

5. Dial-up/Wireless terminals must immediately employ, at a minimum, a personal/software based firewall. Personal firewalls shall meet the requirements stated in the section 1.9.9.A. Wireless devices procured before April 30, 2007 do not require a personal/software based firewall until September 30, 2010.
- B. All data accessed via the 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 the CLETS by utilizing a ciphered User-ID and password ~~security to access the communications server~~ meeting the requirements stated in Section 1.9.8 to access the communications server. ~~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.~~ Encryption shall meet the requirements stated in section 1.9.6.
  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.~~

## DOJ RATIONALE

- 1.6.9 Dial-up/Wireless Access to the CLETS – As the CA DOJ currently receives the Dial-up and Wireless applications and has a process in place for approval, all references to the CAC approving the applications were modified to reflect the current approval process by the CA DOJ. This is consistent with the modification made to section 1.3.2. In addition, the reference to the CLETS Technical Guide was removed. The updated sections for passwords and encryption requirements are referenced.

## FIELD COMMENTS

- 1.6.9.A.5 - Has this gone out in an Information Bulletin or other method?
- Move Wireless to another section
- First sentence – change or delete “normally”

## 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 the CLETS. MSCs shall be maintained with a 98% availability and up-time measured over a continuous ~~twelve~~ 12 month period, including all (scheduled and unscheduled) downtime.

- A. All direct interface MSCs shall record all transactions to and from the CLETS in their entirety on an automated log or journal, and shall have the capability to search and print all journals for a three year period. The journals shall identify the ~~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~~ that also identify the requester and secondary recipient shall meet criminal history offender record information audit requirements. A secondary optional field located after the text should be used to identify a requester other than the CLETS terminal operator.
- B. All ~~message switching computers~~ MSCs interfaced with the CLETS must follow ~~the CLETS Computer Interface Rules and Requirements (R&Rs)~~ the requirements adopted by the ~~CLETS Advisory Committee CA DOJ and the FBI's CJIS Security Policy~~ 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.~~

### DOJ RATIONALE

- 1.7.1 Message Switching Computer (MSC) Definition and Requirements – Section B – The references to the CLETS Computer Interface Rules and Requirements as well as the reference to these rules & requirements being adopted by the CAC were deleted. Requirements are based on CA DOJ policy, which is approved by the CAC, and the FBI's CJIS Security Policy which must be followed by all states.

### FIELD COMMENTS

## 1.7.2 ~~Message Switching Computer~~ MSC 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 upgrade or relocate must formally advise the CA DOJ ~~CLETS Executive Secretary~~ at least 60 90 days in advance of the move with the new address, planned move/implementation date, and if test lines and terminal mnemonics are required.

### DOJ RATIONALE

- 1.7.2 – MSC Design – The reference to the CAC was removed to be consistent with section 1.3.2. As previously stated, the CA DOJ has a 7 tier approval process for new applications and a 5 tier approval process for upgrade applications which includes approvals of circuitry, switching devices and interface equipment.

### FIELD COMMENTS

### 1.7.3 System Upgrade

An upgrade consists of any installation, replacement, or planned enhancement that has a direct impact on the CLETS by ~~of a directly or indirectly connected host server by~~ of a CLETS subscriber subscribing 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 subscribing agency shall forward the a completed upgrade application to the County Control Agency/Direct Interface System Host for review and recommendation (see Section 1.4.1 1.4.3 and 1.4.4). The County Control Agency/Direct Interface System Host shall send the application along with comments will be addressed to the CLETS Advisory Committee CA DOJ 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 the 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~~ see Exhibit H). The County Control Agency must certify that each of the CLETS subscribers subscribing agencies 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.

## DOJ RATIONALE

- 1.7.3. System Upgrade – Section A - All references to the CLETS Executive Secretary and the CAC were deleted. The CA DOJ has a comprehensive approval process in place for reviewing and approving the upgrade applications as cited in section 1.3.2.

## FIELD COMMENTS

- 1.7.3.A - Removal of language regarding the process of upgrades: "...shall send the application along with comments to the CLETS Advisory Committee through the CLETS Executive Secretary...Changes to the application should be in writing. Should any request for... increase CLETS cost or depart from ...the CLETS Advisory Committee shall have the final say."

There should remain policy related to this issue

- section B hardware/software vendor & communications vendor are the same – make communications/software vendor.
- Examples of system diagram – these are sent back too often. Have workshops of how to diagram system.

#### 1.7.4 ~~Message Switching Computer~~ MSC Test Lines

An agency upgrading its system may need to conduct testing prior to production implementation. Once an upgrade application has been approved by the ~~CLETS Advisory Committee~~ CA DOJ, the agency must request a test line and any test mnemonics in writing from the CA DOJ ~~CLETS Executive Secretary~~. During the testing period of a new or upgraded system, the agency is responsible for the line, equipment (Channel Service Units/Data Service Units, 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~~ CA DOJ.

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

#### FIELD COMMENTS

- CSU/DSU terminology outdated
- Clarify who is responsible for managing encryption - DOJ is responsible for encryption to agency whether test or live.

## **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 their local users on how to access the MSC and the use of pre-formatted screens.

## **FIELD COMMENTS**

### 1.8.32 Database Training

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

- A. It is the responsibility of all city, county, state, and federal agencies that use information supplied data accessed via the CLETS to participate in the Department of Justice's CA 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~~ regulations of each file that is accessed or updated. Training shall be provided only by the Department of Justice's Field Operations Program CA DOJ's training staff or another certified CLETS/NCIC trainer.

Specifically, the training requirements are as follows:

1. Initially (within six months of employment or assignment) train, functionally test, and affirm the proficiency of all terminal (equipment) operators (full access/less than full access) ~~in order~~ to ensure compliance with the CLETS/NCIC policies and regulations. This is accomplished by completing the required training and the appropriate CLETS/NCIC Telecommunications Workbook Proficiency Examination published by the Department of Justice CA DOJ, or a facsimile thereof. An agency wishing to make additions or modifications to the ~~Workbook~~ Proficiency Examination must receive prior approval from the Department of Justice, Field Operations Program CA DOJ.
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 the 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 CA DOJ, 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 CA DOJ.

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.~~ Training records, written or electronic, shall identify the employee's CLETS category of Full Access operator, Less Than Full Access operator, Practitioner or Administrator. The records must record the date of initial CLETS training, and for operators, the date the Telecommunications Proficiency Examination was completed, recording a passing score of 70% or better, or a pass/fail notation. ~~The workbooks and exams~~ Examinations may be discarded returned to the operator upon entry of the required information in the appropriate log. An individual's CLETS training record may be deleted one year after they have separated from the agency.
  4. Initially (within 6 months of employment or assignment) all sworn/non-sworn practitioner personnel must receive basic training in the CLETS/NCIC ~~policy~~ policies and regulations.
  5. Make available appropriate training on the CLETS/NCIC system use for criminal justice practitioners other than sworn personnel.
  6. All sworn law enforcement personnel and other practitioners should be provided with continuing access to information concerning the CLETS/NCIC systems, using methods such as roll call and in-service training.
  7. Provide peer-level training on the CLETS/NCIC system use, regulations, policies, audits, sanctions, and related civil liability for criminal justice administrators and upper-level managers.
- B. To ensure compliance with this training mandate, the ~~Department of Justice~~ CA DOJ 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~~ may be conducted by ~~Department of Justice~~ CA DOJ staff.

## FIELD COMMENTS

- Put in writing the requirements for the SPOC training, if any.

- Need to expand on what is required for practitioner or administrator training.

### **1.8.3 Security Awareness Training**

Initially (within 6 months of employment or assignment) all new employees who have access to the CLETS equipment or data accessed via the CLETS, including all appropriate Information Technology personnel, shall receive security awareness training. Thereafter, all personnel who manage or have access to the CLETS equipment or data accessed via the CLETS shall receive security awareness training at a minimum of once every three years. Documentation pertaining to the materials used and those employees who have received security awareness training shall be maintained in a current status.

#### **DOJ RATIONALE**

- 1.8.3 Security Awareness Training – The requirement for security awareness training was added to comply with the FBI's CJIS Security Policy section 4.3.

#### **FIELD COMMENTS**

- Section 1.8.3 - Security Awareness Training should be defined before it's placed in the PPP. The 3 year requirement is different from our current two year Operator Proficiency Exam schedule. Is this training satisfied by the current CLETS training and proficiency exam process?
- Section 1.8.3 Security Awareness Training: This is a good policy and I'm glad to see it added. The documentation of same will be another burden to the ATC or SPOC, whoever this falls under, but the practice is good!
- What is this training? Why is this a CLETS issue?
- Notify POST of Security Awareness requirements. They should be teaching this in their academy. Some agencies hire people with POST certificates and don't do their own training because they assume POST has done it.

## 1.9 SECURITY

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

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

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

## FIELD COMMENTS

### 1.9.1 Location of Terminals and Equipment

Pursuant to the FBI's CJIS Security Policy section 4.4.1, 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 data accessed via the 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 immediately notify the CA DOJ CLETS Executive Secretary of the terminal mnemonic and ~~originating agency identifier (ORI)~~ whenever a terminal is suspected of being stolen or misplaced.

### FIELD COMMENTS

### **1.9.2 Background and Fingerprint Requirements *Fingerprint Based Criminal Offender Record Information Search***

- A. All persons, including non-criminal justice, volunteer personnel, and private vendor technical or maintenance personnel, with physical access to the CLETS equipment, provided information data accessed via the CLETS or to ~~Criminal Offender Record Information (CORI)~~, are required to undergo a background and fingerprint check based criminal offender record information search pursuant to the California Code of Regulations, Title 11, Division 1, Chapter 7, Article 1, Subsections 703(d) and 707(b).
- ~~1.~~ 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.
  21. Where the CLETS access is available without ~~CORI~~ criminal offender record information, all persons, including non-criminal justice and private vendor technical or maintenance personnel, accessing areas where the CLETS equipment or CLETS information data accessed via the CLETS is located are required to undergo a background and fingerprint check based criminal offender record information search.
  32. Pursuant to the FBI's CJIS Security Policy section 4.5, ~~if~~ if the background/fingerprint based check criminal offender record information search reveals a felony conviction of any kind, CLETS/NCIC access shall not be granted. If it is revealed that the person appears to be a fugitive or has an arrest history without conviction for a felony, the ~~criminal justice~~ agency head, or his/her designee will review the matter and decide if the CLETS system access is appropriate.
  43. Visitors to a computer center, such as a tour group, where the computer center has ~~CORI~~ criminal offender record information access are not required to undergo a background and fingerprint

based check criminal offender record information search. They must, however, be escorted at all times.

54. The final responsibility for maintaining the security and confidentiality of criminal justice information rests with the individual agency head or administrator.

B. Personnel authorized terminal access to the CLETS may be sworn law enforcement or criminal justice personnel, non-sworn law enforcement or criminal justice personnel, or non-criminal justice, volunteer personnel, and private vendor technical or maintenance personnel that who 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) A CA DOJ fingerprint check based criminal offender record information search.

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

2. An FBI fingerprint check based criminal offender record information search

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 is 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

43. Department of Justice Additionally, the CA DOJ CJIS criminal justice databases may be accessed for background investigation of law enforcement and criminal justice employees, with the exception of the Automated Criminal History and Mental Health Firearms Prohibition Systems., for background investigations of

~~law enforcement and 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 the CLETS terminals, equipment or information until a background and fingerprint check based criminal offender record information search is completed and approved by the agency head. Following approval of the completed investigation, a memorandum or other notation should be placed either in the employee's personnel file or in another pertinent file indicating that authorization has been granted.

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

## DOJ RATIONALE

- 1.9.2 Fingerprint Based Criminal Offender Record Information Search – Section 1.9.2.B.1. Note - This note was deleted because the FBI's CJIS Security Policy 4.5.1.a. allows a federal entity to omit a state fingerprint-base criminal offender record information search when the federal agency bypasses the state repositories. All federal agencies with the CLETS access also have access to state repositories; therefore, federal agencies must comply with section 1.9.2.B.1 & 2. Section 1.9.2.B.2. Note – This note was deleted because the FBI's CJIS Security Policy states that authorized personnel are those persons who have passed a state and FBI fingerprint-based criminal offender record information search and have been granted access to the databases. There is no mention of an exemption for temporary employees. Section 1.9.2.B.3 – This section was deleted because agencies can set their own policies on what additional background searches they require for employees.

## FIELD COMMENTS

- 1.9.2.B.1 - Federal agencies are no longer exempt?
- Put the word "background" back in the title. Agencies need this to do more than just a fingerprint check.
- Add back in that an agency can go above and beyond fingerprints.

### 1.9.3 User Access

- A. It is required that each employee/volunteer sign an employee/volunteer statement form prior to operating or having access to the CLETS terminals, equipment, or information. It is recommended that each employee/volunteer sign an employee/volunteer statement form on a biennial basis. Additional requirements may be added at an agency's discretion. Any addition cannot negate the intent of the Employee/Volunteer Statement Form. (See **Exhibit I** for a sample Employee/Volunteer Statement Form.)
- B. All logins, successful and unsuccessful must be logged. Repeated failed log on attempts shall disable the user account. All logging must meet the requirements stated in section 1.9.5. ~~Such logs must be retained by the agency for three years.~~
- C. When a person with access to the CLETS is no longer employed or no longer accessing the CLETS on behalf of the law enforcement or criminal justice agency, the agency is responsible for removing all related passwords, security authorizations, tokens, etc., from the system.

### FIELD COMMENTS

- Section 1.9.3 - The term "repeated" needs to be defined. During CLETS Inspections we are always asked how many failed logon attempts make up "repeated". Is it three, five or 21?

#### **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 that meets 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 section 1.9.6.
  - 3. Two factor authentication shall be used where at least one factor meets the Advanced Authentication standards identified in the FBI's CJIS Security Policy section 7.3.
  - 4. The VPN equipment resides behind a network firewall that meets the requirements stated in section 1.9.9.
  - 5. Terminals with the CLETS access shall employ, at a minimum, a personal/software based firewall. Personal firewalls shall meet the requirements stated in section 1.9.9.
  - 6. Only agency owned and/or authorized computer systems shall be used. Personally owned systems shall not be used.
- C. A terminal with the CLETS access shall not access the Internet unless that access is protected by a network firewall that meets the requirements specified in section 1.9.9.

#### **FIELD COMMENTS**

- Regarding 1.9.4: This section refers to the FBI's CJIS Security Policy sections 7.3/7.3.1. Can this be included as an Exhibit in the PPP's?

### **1.9.5 Logging**

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

### **DOJ RATIONALE**

- 1.9.5 Logging – Logging requirements were added to be in compliance with the FBI's CJIS Security Policy.

### **FIELD COMMENTS**

- Section 1.9.5 Logging: The new policy reflects the wrong FBI CJIS Security Policy section. It should be 7.11, not 8.4. Second, this new requirement lists "file access and type of transactions and password changes" These specifics were not included in the last version of the PPP. I would suspect that not all agencies have set up their logging to include all these things. How long will everyone have to catch up to these extended requirements that were not requirements before?

### **1.9.6 Encryption**

Data accessed via the CLETS and transmitted through any public network segment, wireless network, untrusted network or the public Internet shall be immediately protected with encryption. The encryption shall meet the requirements specified in the FBI's CJIS Security Policy section 7.8.

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

### **DOJ RATIONALE**

- 1.9.6 Encryption – Encryption requirements were added to be in compliance with the FBI's CJIS Security Policy.

### **FIELD COMMENTS**

- Section 1.9.6 Encryption: The second paragraph speaks of an agency managing their encryption keys. Perhaps this can or should be worded to include that these keys can be managed or handled to the non-CJ who is mentioned in our Management Control Agreement. In our case, County ITD manages all software and encryption keys, and we prefer it that way.

### **1.9.7 Virus Protection**

All systems with the CLETS connectivity or access to data accessed via the CLETS shall employ virus protection software that meets the requirements stated in the FBI's CJIS Security Policy section 7.12.

#### **DOJ RATIONALE**

- 1.9.7 Virus Protection – Virus protection requirements were added to be in compliance with the FBI's CJIS Security Policy.

#### **FIELD COMMENTS**

### **1.9.8 Authentication**

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

A. Where passwords are used to authenticate users, those passwords shall meet the requirements stated in the FBI's CJIS Security Policy section 7.4.2.3.

B. Where advanced authentication is required (such as receiving data accessed via the CLETS over the Internet), the advanced authentication shall meet one of the approved methods as described in the FBI's CJIS Security Policy section 7.3.

### **DOJ RATIONALE**

- 1.9.8 Authentication - Authentication requirements were added to be in compliance with the FBI's CJIS Security Policy.

### **FIELD COMMENTS**

### **1.9.9 Firewalls**

Firewalls are implemented to provide a point of defense, control and audit access to the CLETS equipment and data accessed via the CLETS. Where firewalls are required, those firewalls shall meet the requirements as stated in the FBI's CJIS Security Policy section 7.10.

#### **A. Personal Firewalls**

A personal firewall is defined as a firewall that can operate with only one network interface. Personal firewalls are required for wireless devices and shall meet the requirements specified in the FBI's CJIS Security Policy section 7.10.2.

### **DOJ RATIONALE**

- 1.9.9 Firewalls - Firewall requirements previously in section 1.9.4, were updated to be in compliance with the FBI's CJIS Security Policy and moved to its own section.

### **FIELD COMMENTS**

### **1.9.10 Handheld Devices**

Handheld devices used to receive data accessed via the CLETS are permitted if the following additional requirements are met. The handheld devices referenced here include, but are not limited to, Personal Digital Assistants, Personal Electronic Devices, cellular phones, smart phones and other multifunction handheld devices.

A. A handheld device shall incorporate a personal firewall. A personal firewall is defined as a firewall that can operate with only one network interface on a personal computer or other handheld computing device. Personal firewalls shall meet the requirements specified in the FBI's CJIS Security Policy section 7.10.2.

B. Data accessed via the CLETS shall not be stored unprotected on handheld or portable media devices. Data accessed via the CLETS and stored on handheld or portable media devices shall have all residual data protected by encryption or erasure. Encryption shall meet the requirements stated in section 1.9.4.

### **DOJ RATIONALE**

- 1.9.10 Handheld Devices – Handheld device specifications were added along with security requirements as required by the FBI's CJIS Security Policy.

### **FIELD COMMENTS**

### **1.9.11 Media Disposal**

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

### **DOJ RATIONALE**

- 1.9.11 Media Disposal – Media disposal requirements were added to be in compliance with the FBI's CJIS Security Policy.

### **FIELD COMMENTS**

### **1.9.12 Patch Management**

All systems and devices with the CLETS connectivity or access to data accessed via the CLETS shall use manufacturer supported software and firmware. All software and firmware shall be kept up to date with all critical security patches.

### **DOJ RATIONALE**

- 1.9.12 Patch Management – Patch management requirements were added to maintain the security of the host device and the CLETS.

### **FIELD COMMENTS**

- Add that exemptions to this requirement must be submitted to DOJ/CAC.

## 1.10 SYSTEM DISCIPLINE/APPEAL PROCESS

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

### DOJ RATIONALE

- 1.10 System Discipline/Appeal Process – The CAC was removed as the responsible party for conducting random sampling. The CA DOJ employees regularly visit the user agencies and, through random sampling, audit various activities to determine the agencies conformity with the CLETS policies and regulations.

### FIELD COMMENTS

### 1.10.1 System Misuse

- A. Violation of CLETS ~~the CA DOJ rules, regulations, or and policies and regulations, practices, and procedures~~ shall be investigated by the ~~CLETS Executive Secretary~~ agency head. 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 recommend on a course of action or sanction to apply. The CLETS Executive Secretary will issue a letter formally notifying the agency of the decision.~~

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

- B. In the event of A a violation of law (government or penal code) or CLETS ~~the CA DOJ rules, regulations, or policies and regulations, practices, and procedures~~ may result in system misuse, any of the following sanctions, dependent upon the total circumstances of the incident: the CA DOJ will take appropriate action such as:
1. Letter of censure;

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

## DOJ RATIONALE

- 1.10.1 System Misuse – This section was rewritten to allow agencies to investigate their own suspected misuse. In accordance with section 1.7.1, the MSC is required to journal all CLETS transactions; therefore, an agency has access to system misuse data. In the event that the CA DOJ is needed to conduct a journal search, the requirements are provided in this section. The agency head will be responsible for investigating and resolving any system misuse.

## FIELD COMMENTS

- Deleted Section / 1.10.1.D - Why was the misuse reporting requirement eliminated? This is a tool to evaluate potential problems with the CLETS that might need to be addressed.
- Section 1.10.1 System Misuse old section D - I am surprised that CAS no longer desires a yearly report of misuse from the agencies. The CAC always seemed to want to know these numbers and the results.
- 1.10.1.A - The language added regarding “The agency head shall investigation...” and further refers to a journal search request, states: “...request on agency letterhead, signed by a supervisor or agency head...” This is the ATC’s job, so why are they not listed?

It is unclear why some things are not allowed via the ATC, but then all compliance items are expected to be handled solely by the ATC. This is a natural area for the ATC to handle, and the ATC should be authorized to request this search. Likewise, the response should go back to the requester, not to the agency head (it could easily get lost in a larger agency).

- All language removed as to CAC having any oversight in CLETS misuse issues.
- The agency head or his/her designee should be added to 1.10.1A.

### **1.10.2 Discontinuance of the CLETS Service**

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

## GENERAL CHANGE COMMENTS

- All variation of rules, regulations, policies, practices & procedures were changed to policies and regulations: I disagree with this change. The CLETS PPPs have been the Bible we used forever for guidance, and this is how the users know the document.
- Sometimes reference is to Direct Interface Host System; sometimes it's Direct Interface System Host.
- The DOJ has removed all references to the CLETS Advisory Committee (CAC) having any authority, approval, decisional or other type of active role with user agencies. This would include areas of policy changes, user approval and discipline, meeting requirements (posting notices, etc.).

Some changes are found in replacing "the CAC" with "the DOJ" in the language and some are in replacing "the CLETS Executive Secretary" with "the DOJ."

- Removing CAC authority for all specified areas should be reversed. There would be a definite conflict of interest if DOJ had full and final say of all rules and regulations (including the ability to change them without CAC input or approval) and user issues.
- Although many changes were only made to replacing language referencing the CLETS Executive Secretary (a DOJ employee), this would still have a huge impact. Although many of the items sent to the CLETS Executive Secretary are completed by the DOJ with no CAC input or activity, the fact that the item is for the CLETS Executive Secretary's approval still places overall approval, and any subsequent problems with the approval, at the CAC level, which is needed by the user community.

CAC is intended, (according to GC 15154), to advise and assist in the management of the system with respect with operating policies, service evaluation, and system discipline. Changing all references to DOJ instead of CAC is contrary to the direction of this GC section. What would be the purpose of CAC meetings (which would still be mandated by this code section)?

Users have historically had a difficult time in getting assistance or issues heard at the DOJ level, and the most contributing factor in obtaining resolve has been that the issue either was going, or could go, to the CAC for final approval.

Additionally, as seen typically with any agency re-organization or staffing and/or budget issues/changes, many things can be placed on the back burner. Placing everything with DOJ's approval could adversely affect an agency due to this.