

**ATTACHMENT to the CLETS POLICIES, PRACTICES and PROCEDURES**  
**DRAFT VERSION DATED JULY 30, 2008**

**Rationale for suggested changes to**  
***The CLETS Policies, Practices and Procedures***  
**to be presented at the October 16, 2008, CAC meeting**

Throughout the California Law Enforcement Telecommunications Systems (CLETS) Policies, Practices and Procedures (PPPs), wherever possible, reference has been made to the applicable sections of the Federal Bureau of Investigation's (FBI's) Criminal Justice Information Services (CJIS) Security Policy, which is the guiding policy the California Department of Justice (CA DOJ) must follow. Reference is also made to applicable PPP sections.

- Language was standardized throughout the document:
  - DOJ was changed to CA DOJ as to not have confusion between the state and federal Department of Justice;
  - Background check and fingerprint check were changed to fingerprint based criminal offender record information;
  - CLETS data, CLETS-provided data, CLETS information were changed to data accessed via the CLETS;
  - Criminal Justice Information Systems (CJIS) databases was changed to CA DOJ criminal justice databases to minimize the confusion between it, the federal CJIS and the California Justice Information Services (CJIS) Division of the CA DOJ;
  - All variations of rules, regulations, policies, practices & procedures were changed to policies and regulations;
  - Subscriber agency and subscriber were changed to subscribing agency.
  
- Section 1.1 Purpose and System Description – This section was condensed to reflect what is written in the statutes pertaining to the CLETS.
  
- 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.
  
- 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.

- 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.
- 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 seven tiered approval process for new applications and a five 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.

- 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.
- 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.
- 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.

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.

- 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.
- 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.
- 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.
- 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.
- 1.9.5 Logging – Logging requirements were added to be in compliance with the FBI's CJIS Security Policy.
- 1.9.6 Encryption – Encryption requirements were added to be in compliance with the FBI's CJIS Security Policy.
- 1.9.7 Virus Protection – Virus protection requirements were added to be in compliance with the FBI's CJIS Security Policy.
- 1.9.8 Authentication - Authentication requirements were added to be in compliance with the FBI's CJIS Security Policy.

- 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.
- 1.9.10 Handheld Devices – Handheld device specifications were added along with security requirements as required by the FBI's CJIS Security Policy.
- 1.9.11 Media Disposal – Media disposal requirements were added to be in compliance with the FBI's CJIS Security Policy.
- 1.9.12 Patch Management – Patch management requirements were added to maintain the security of the host device and the CLETS.
- 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.
- 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.