California Department of Justice
CLETS Policy and Security Audit Questionnaire

Agency Name	**Main ORI Number**	**County**
Agency CLETS Coordinator (ACC)	Email Address	Telephone Number
Fax Number	Physical Address	Mailing Address
Person Completing Audit (if not ACC)	Title	Telephone Number
Fax Number	Email Address	Mailing Address
SPOC ☐ Check if same as ACC	Email Address	Telephone Number
Fax Number	Physical Address	Mailing Address
Head of Agency	Title	Appointment Date
Telephone Number	Physical Address	Mailing Address
Email Address	Fax Number	

Section 1: Agency Information

FBI CJIS Security Policy 5.9: Physical Protection

1. The attached Terminal Location Spreadsheet (TLS) is **required**. Complete the TLS and return with the audit. The spreadsheet will provide your auditor with more information on your terminals, their physical location and assist in determining which locations will receive a site visit. *Information provided below should match your TLS.

☐ Agency completed TLS with all ORI's and physical addresses listed

2. Total number of physical addresses* with access to CLETS _____

Total number of computers* with the ability to access Criminal Justice Information (CJI) _____

Total number of wireless devices with CLETS access (include MDT, laptops, tablets, smart phones, etc.) _____

3. Does your agency have vehicles with CLETS access? ☐ Yes ☐ No

If yes, how are these devices mounted?

☐ Fixed ☐ Removable ☐ Both

4. Are personal/software based firewalls employed on mobile devices with access to Criminal Justice Information (CJI) (i.e. laptops, tablets, smart phones, etc.)? (FBI CJIS Security Policy 5.13.4.3)

☐ Yes ☐ No ☐ No mobile devices

5. Is a Mobile Device Management (MDM) system used to manage mobile devices?
(i.e. Apple or iOS devices) (FBI CJIS Security Policy 5.13.2)

☐ Yes ☐ No ☐ No mobile devices

6. Does your agency have advanced authentication in place for devices with access to CJI that are not in a physically secure location? (i.e. Windows, Android, LINUX, etc.)
(FBI CJIS Security Policy 5.6.2.2.1)

☐ Yes ☐ No ☐ No mobile devices

Note: Each answer box has maximum characters allowed. If you need additional space to provide your answers, please attach a document and note the Section and Question numbers so the auditor can review the entire submission.

Section 2: Account Management and Security

(CLETS PPP sections 1.4 through 1.7, and 1.9)

1. How does your agency access CLETS? Check all that apply.

- ☐ County Control Agency (PPP 1.4.4)
- ☐ Direct Interface System Host (PPP 1.4.5)
- ☐ Local Agency Direct Interface (PPP 1.4.6)
- ☐ DOJ LEAWEB

2. If your agency is a host, list the agencies that access your CLETS interface.

3. Has a unique user ID and password been assigned to each CLETS user? (PPP 1.6.7B)

☐ Yes ☐ No

4. Are CLETS user IDs **reassigned** to a different user within six-months of their last use?(PPP 1.6.7 B)

☐ Yes ☐ No

5. If passwords are used to authenticate an individual's unique ID, are all of the following basic password standards met: 1) be a minimum length of eight (8) characters on all systems; 2) not be a dictionary word or proper name; 3) not be the same as the User ID; 4) expire within a maximum of 90 calendar days; 5) not be identical to the previous ten (10) passwords; 6) not be transmitted in the clear outside the secure location; 7) not be displayed when entered?
(FBI CJIS Security Policy 5.6.2.1.1)

☐ Yes ☐ No ☐ Advanced Password Standards used per FBI CJIS Security Policy 5.6.2.1.2

6. Has your agency conducted the required CA and FBI fingerprint security background checks on all sworn/non-sworn personnel, volunteers, consultants, maintenance/janitorial personnel, shred companies, vendors, etc. who have **unescorted access** to CJI (i.e. anyone who can view, hear or touch CLETS, CORI, III, etc.)? (FBI CJIS Security Policy 5.12 and PPP 1.9.2 A, B & C)

☐ Yes ☐ No ☐ Some, not all (Explain Below)

Note: Each answer box has maximum characters allowed. If you need additional space to provide your answers, please attach a document and note the Section and Question numbers so the auditor can review the entire submission.

7. Are personnel allowed to operate CLETS devices or equipment, or access CLETS information, CORI or III, before a fingerprint security background investigation is completed and approved by the agency head or designee? (FBI CJIS Security Policy 5.12 and PPP 1.9.2)

☐ Yes ☐ No

8. Has each employee or volunteer signed a Employee/Volunteer Statement prior to operating or having access to CLETS terminals, equipment, or information? (PPP 1.9.3A)
Submit a few random signed sample copies your agency's Employee/Volunteer Statement forms for verification purposes.

☐ Yes (Attached) ☐ No

9. Do all CLETS access devices automatically lock a user out of a session after a period of inactivity (30 minutes or less) with the exception of being, (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e. receive only terminals) used within physically secure location facilities that remain staffed when in operation? (FBI CJIS Security Policy 5.5.5)

☐ Yes ☐ No

10. Provide a screen print or picture of all agency CLETS terminal System Use Notification message(s). (FBI CJIS Security Policy 5.5.4)

☐ Attached

11. How does your agency verify and document CLETS user accounts? Include **who** completes and **how often**. (FBI CJIS Security Policy 5.5.1 PPP 1.9.3B)

12. When a person with CLETS access is no longer a CLETS user, what is the procedure for deleting the person's CLETS access and what is the time frame? (FBI CJIS Security Policy 5.5.1 PPP 1.9.3B and C)

Note: Each answer box has maximum characters allowed. If you need additional space to provide your answers, please attach a document and note the Section and Question numbers so the auditor can review the entire submission.

13. Does your agency have malicious code protection that includes automatic updates for all systems with Internet access and employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all work stations, servers, and mobile computing devices on the network? (FBI CJIS Security Policy 5.10.4.2)

☐ Yes ☐ No

14. Does your agency designate an individual or position to review/analyze the computer system (including hardware, software, system users and data) audit records for indications of inappropriate or unusual activity, investigate suspicious activity, or suspected violations? Audit review/analysis shall be conducted at a minimum once a week. (FBI CJIS Security Policy 5.4.3)

☐ Yes ☐ No

15. Does your agency ensure any connections to other external networks, information systems, or the Internet occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, encrypted tunnels)? (FBI CJIS Security Policy 5.10.1.1)

☐ Yes ☐ No

Note: Each answer box has maximum characters allowed. If you need additional space to provide your answers, please attach a document and note the Section and Question numbers so the auditor can review the entire submission.

Section 3: Administrative Security (FBI CJIS Security Policy 5.1.1.5 & PPP 1.5.1)

1. Please list all companies/agencies/contractors/vendors/city/county/state/govt. contractors that have **unescorted** access to your secure facility/network. Examples: janitorial, IT services, shred companies, jailers, mental health, medical, and religious providers, property managers, facilities, social services, public works, food vendors, lock smiths, etc. Check the boxes below indicating that the required items are completed and included.

☐ **N/A - All vendors and contractors are escorted at all times**

Provider Name: _____ **Services Provided:** _____

Required Items:

☐ Management Control Agreement (MCA) - required for city or county contractors

or

☐ Private Contractor Management Control Agreement (PCMCA) - required for private contractors/vendors and it's employees

☐ Signed Security Addendum (Required for PCMCA only)

☐ Fingerprinted - CA & FBI level & approve by agency head

☐ Security Awareness Training

☐ Signed Employee/Volunteer Statement

Comments:

Provider Name: _____ **Services Provided:** _____

Required Items:

☐ Management Control Agreement (MCA) - required for city or county contractors

or

☐ Private Contractor Management Control Agreement (PCMCA) - required for private contractors/vendors and it's employees

☐ Signed Security Addendum (Required for PCMCA only)

☐ Fingerprinted - CA & FBI level & approve by agency head

☐ Security Awareness Training

☐ Signed Employee/Volunteer Statement

Comments:

Copy page 7 if you need to add more companies/vendors.

Note: Each answer box has maximum characters allowed. If you need additional space to provide your answers, please attach a document and note the Section and Question numbers so the auditor can review the entire submission.

Provider Name: _____ **Services Provided:** _____

Required Items:

- ☐ Management Control Agreement (MCA) - required for city or county contractors

or

- ☐ Private Contractor Management Control Agreement (PCMCA) - required for private contractors/vendors and it's employees
- ☐ Signed Security Addendum (Required for PCMCA only)
- ☐ Fingerprinted - CA & FBI level & approve by agency head
- ☐ Security Awareness Training
- ☐ Signed Employee/Volunteer Statement

Comments:

Provider Name: _____ **Services Provided:** _____

Required Items:

- ☐ Management Control Agreement (MCA) - required for city or county contractors

or

- ☐ Private Contractor Management Control Agreement (PCMCA) - required for private contractors/vendors and it's employees
- ☐ Signed Security Addendum (Required for PCMCA only)
- ☐ Fingerprinted - CA & FBI level & approve by agency head
- ☐ Security Awareness Training
- ☐ Signed Employee/Volunteer Statement

Comments:

Copy this page if you need to add more companies/vendors.

Note: Each answer box has maximum characters allowed. If you need additional space to provide your answers, please attach a document and note the Section and Question numbers so the auditor can review the entire submission.

Section 4: Record Management

1. Does your agency release CLETS provided information to a **non-subscribing agency** (i.e., social services agency, housing authority, code enforcement, etc.)? (PPP 1.5.3)
If yes, list the non-subscribing agency(ies)

☐ Yes ☐ No

Non-Subscribing Agency:	Release of Information Form (CLETS)	CA/FBI Fingerprint	Security Awareness Training	Signed Employee/ Volunteer Statement
_____	☐	☐	☐	☐
_____	☐	☐	☐	☐
_____	☐	☐	☐	☐

If applicable, attach list of additional Non-Subscribing agencies not listed above. ☐ Attached

2. Has your agency placed a CLETS terminal or mnemonic with another governmental agency (i.e., family support, code enforcement, etc.)? (PPP 1.5.2)
If yes, list the agency(ies)

☐ Yes ☐ No

Non-Subscribing Agency:	CLETS Interagency Agreement	CA/FBI Fingerprint	Security Awareness Training	Signed Employee/ Volunteer Statement
_____	☐	☐	☐	☐
_____	☐	☐	☐	☐
_____	☐	☐	☐	☐

If applicable, attach list of additional agencies not listed above. ☐ Attached

Note: Each answer box has maximum characters allowed. If you need additional space to provide your answers, please attach a document and note the Section and Question numbers so the auditor can review the entire submission.

3. If your agency enters records or conducts hit confirmation for another agency or another agency enters records or conducts hits confirmations for your agency, provide a Reciprocity Agreement. (PPP 1.5.4)

☐ Attached ☐ Inquiry Only/No Hit Confirmations ☐ N/A

4. How does your agency dispose of CLETS/CORI/III information in hard copy format when no longer needed? (FBI CJIS Security Policy 5.8.3-5.8.4)

Please Select One

Comments:

5. How does your agency dispose of CLETS/CORI/III information in an electronic format, such as disc, flash drives, hard drives, servers etc., when no longer needed? (FBI CJIS Security Policy 5.8.3-5.8.4)

Please Select One

Comments:

Note: Each answer box has maximum characters allowed. If you need additional space to provide your answers, please attach a document and note the Section and Question numbers so the auditor can review the entire submission.

Section 5: Training (PPP 1.8 and FBI CJIS Security Policy 5.2)

1. All Full and Less than Full Access Operators are required to complete **Initial Training** within the first six months of employment/assignment by a DOJ certified instructor.
List the names of all certified trainers in the box below. Provide initial training logs and a copy of your initial training materials.
Certified Trainer(s) name(s):

☐ Initial training logs attached ☐ Training materials attached

2. Explain how your agency's **Biennial Recertification** training is administered and tracked for all Full Access and Less than Full Access Operators. Submit a copy of a page from your agency's recertification (e.g. nexTEST) training log(s)/report.

3. Does your agency ensure that biennial **Security Awareness** training is provided to all personnel who have access to criminal justice information, including but not limited to: all agency personnel, city/ county janitorial and/or IT staff, and private contractor staff (i.e. anyone who can view, hear or touch CLETS, CORI, III, etc.) (FBI CJIS Security Policy 5.2.)? Submit a copy of a page from your agency's training log, nexTEST report, and/or CJIS Online (Vendors) Report for verification purposes.

☐ Yes ☐ No

4. Have your agency administrators read the "Areas of Liability for the Criminal Justice Information System Administrator"? (PPP 1.8.2 A 7)
Submit a copy of the signature page.

☐ Yes (Attached) ☐ No

5. Are your agency administrators tested at the appropriate level (Full Access, Less than Full, or Practitioner)?

☐ Yes ☐ No

6. Are all CLETS users and practitioners provided with updated information concerning CLETS/NCIC systems, using methods such as roll call, in service training, email, CLEW, etc.?

☐ Yes ☐ No

Section 6: Policies and Procedures

1. Provide a copy of your agency's ***Incident Response Plan*** (IRP). An IRP should be a formal written plan outlining steps taken when an information security event and/or weakness is recognized. (FBI CJIS Security Policy 5.3 and 5.13.5)

☐ Attached and indicate Section 6, Question 1

2. Provide a copy of your agency's policy for securely handling, transporting, storing, and destroying media. A formal ***Media Policy*** is required. (FBI CJIS Security Policy 5.8)

☐ Attached and indicate Section 6, Question 2

3. **Describe** your agency's policies and procedures for the physical security and protection of criminal justice information system hardware, software, and media. (FBI CJIS Security Policy 5.9)

☐ Attached and indicate Section 6, Question 3

4. **Describe** your agency's policies and procedures for ensuring prompt installation of newly released security relevant patches, updates, service packs, and hot fixes. (FBI CJIS Security Policy 5.10.4.1)

☐ Attached and indicate Section 6, Question 4

5. **Describe** your agency's formal sanction process for personnel failing to comply with established system policies and procedures. (FBI CJIS Security Policy 5.12.4)

☐ Attached and indicate Section 6, Question 5

Note: Attach documents and note the Section and Question numbers so the auditors can locate and review the proper submission.

Documents in **bold** are mandatory for all agencies to submit with audit. All other documents are to be submitted if applicable to your agency. Please ensure all documents submitted reflect the proper and **current signatures** of the Head of Agency, ACC and/or SPOC. Documents below can be found on https://clew.doj.ca.gov/csp

- ☐ **Terminal Location Spreadsheet**
- ☐ **Agency CLETS Coordinator (ACC) Responsibility**
- ☐ **Security Point of Contact (SPOC) Agreement**
- ☐ **CLETS Subscriber Agreement**
- ☐ **Samples of signed Employee/Volunteer Statement**
- ☐ **Latest Misuse Report**
- ☐ **System Use Notification Message**
- ☐ **Sample of Full Access and Less Than Full Initial Training Log**
- ☐ **Security Awareness Training Log/Biennial Recertification Log**
- ☐ **Initial Training Materials**
- ☐ **Areas of Liability for the CJIS Administrator Signature Page**
- ☐ **Incident Response Plan (IRP)**
- ☐ **Formal Media Policy**
- ☐ Private Contractor Management Control Agreement
- ☐ Samples of signed CJIS Security Addendum
- ☐ Management Control Agreement
- ☐ Reciprocity Agreement(s)
- ☐ Release of CLETS Form
- ☐ Inter-agency Agreement
- ☐ CLETS Change Request Form
- ☐ Other (Specify)_____

The materials can be returned by mail, fax or secure email to:
California Department of Justice
Client Services Program, CLETS Audits and Inspections Section
ATTN: CLETS Audits
P.O. BOX 160968
Sacramento, CA 95816-0968

Fax: (916) 731-2177
Secure email: CLETSAudits@doj.ca.gov

As the Agency CLETS Coordinator or designee, I certify that the above responses are true and correct to the best of my knowledge.

_____

(Please print) FIRST NAME LAST NAME TITLE

_____

SIGNATURE DATE