DEPARTMENT OF JUSTICE
CLIENT SERVICES PROGRAM
CLETS POLICY AND SECURITY AUDIT QUESTIONNAIRE

Section 1: Audit Description and Instructions

The California Department of Justice (CA DOJ) Criminal Justice Information System (CJIS) California Law Enforcement Telecommunications System (CLETS) Policy and Security Audit Questionnaire is intended to ensure compliance of the rules and regulations that the California Department of Justice and Federal Bureau of Investigation created for agencies connecting to or utilizing criminal justice information. The audit process identifies security controls that must be in place and the personnel screening that is necessary. The process covers physical, administrative, and technical security. It examines topics regarding the proper use and protection of criminal history record information, as well as, the necessary procedures that must be in place for attempted or successful security breaches. All references are to CLETS Policies, Practices and Procedures (PPPs), CJIS Security Policy, and NCIC 2000 Manual which can be found on the California Law Enforcement Website (CLEW). It is encouraged that you have these manuals open when answering this audit.

This audit contains many different styles of questions. For questions that ask for information such as procedures, feel free to copy and paste procedures in the box provided or include it in your fax to DOJ (Attaching files/ documents in the box provided is not an option). There will be questions that ask for a copy of an agreement. To assist you with this task there will be a form available to print with a list of the documents to be submitted via fax at the end of the audit. If you are faxing a document, please indicate "Attached by Fax" in the box provided.

If you have questions or need assistance completing this audit, contact your Field Representative or call (916) 227-3332. A list of field representatives can be found on the CLEW website, click on Client Services Program, CLETS Audits and Inspections Section.

Please review the list of documents on this page and fill out the form in it's entirety. For each document you attach, please check the box. Once complete, submit via fax to your Field Representative. The 'Other' section on the Fax Cover Sheet is reserved for documents such as policies and procedures that did not fit in the space provided to answer those questions.

Section 2: Agency Details

DOJ Use

Agency Name	**ORI Number**	**County**
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
Fax Number	Physical Address	Mailing Address
Email Address	Telephone Number	

Section 3: Physical Security
FBI CJIS Security Policy 5.9

1. Please fill out the attached terminal review spreadsheet and return with your audit. The spreadsheet will provide your auditor with more information on your terminals, their location and assist in determining which locations will receive a site visit.

2. Total number of locations with access to CLETS _____
   Number of terminals with ability to access CLETS _____
   Number of wireless devices (include MDT, cell phones, etc.) _____

3. Do you have vehicles with CLETS terminals?

   ☐ Yes ☐ No

4. If yes, where are the vehicles stored when not in use?

Section 4: Administrative Security

1. Does your agency utilize private contractors/vendors (i.e., shred companies, non-government IT, etc.) to manage or maintain any of the CLETS related devices, systems, or applications?

   ☐ Yes ☐ No

   Please provide a list of all of the companies you do business with, and describe how they access CLETS or CLETS related materials:

2. Is a Private Contractor Management Control Agreement in place between the agencies pursuant to the CLETS Polices, Practices, and Procedures (PPP), section 1.5, and has the private contractor(s) and contractor's employees signed the CJIS Security Addendum pursuant to the FBI CJIS Security Policy 5.1.1.5?

☐ Yes ☐ No

Please provide a copy of the Private Contractor Management Control Agreement(s) and a few random samples of signed CJIS Security Addendum.

3. Does your agency allow unescorted access to facilities that contain CLETS devices or information to a public agency that is neither law enforcement nor criminal justice (i.e., County IT, County janitorial, etc.)? (PPP 1.5.1)

☐ Yes ☐ No

Provide a list of all agencies you do business with and in what capacity they may have access to CLETS or CLETS related materials:

4. Are Management Control Agreement(s) on file?

☐ Yes ☐ No ☐ N/A

Please provide a copy of the Management Control Agreement(s) for each business.

Section 5: Account Management and Security

1. How does your agency access CLETS?

Please Select One

If other, specify what Interface or host server your agency is using

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

3. Have there been any upgrades since your last CLETS approved application?(PPP 1.7.3.A)

☐ Yes ☐ No

If yes, have the upgrades been approved by the CLETS Administration Section (CAS) or are they in process?

Please Select One

4. Does your agency pool mnemonics? (PPP 1.6.2 B)

☐ Yes ☐ No

Was the mnemonic pooling application addendum submitted to CAS?

☐ Yes ☐ No ☐ N/A

Please provide a copy of the mnemonic pooling application that was sent to CAS. Indicate the access control point below:

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

☐ Yes ☐ No

6. Are any user ID's being reassigned within six-months of their last use? (PPP 1.6.7 B.)

☐ Yes ☐ No

7. If passwords are used to authenticate an individual's unique ID, are all of the following password requirements 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

8. Are personal/software based firewalls employed on mobile devices (i.e., laptops, handhelds, smartphones, etc.)? (FBI CJIS Security Policy 5.13.4.4.)

☐ Yes ☐ No ☐ N/A

9. Has your agency conducted fingerprint security background checks (CA DOJ and FBI) on all sworn/non-sworn personnel, volunteers, consultants, maintenance/janitorial personnel, shred companies, vendors, etc. who have unescorted access to CLETS, CORI, and/or III Information? (FBI CJIS Security Policy 5.12 and PPP 1.9.2 A, B & C)

☐ Yes ☐ No ☐ Some, not all (explain below)

10. 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? (FBI CJIS Security Policy 5.12 and PPP 1.9.2 A, B & C)

    Please Select One

11. Has each employee or volunteer signed an Employee/Volunteer Statement prior to operating or having access to CLETS terminals, equipment, or information? (PPP 1.9.3 A.) (Recommended to update/review on a biennial basis)

    Please select one

    Submit a few random sample copies of your agency's Employee/Volunteer Statement forms for verification purposes via fax.

12. Are all logons (successful/unsuccessful) being logged and retained for at least one year? (FBI CJIS Security Policy 5.4.6)

    ☐ Yes ☐ No

13. Do repeated failed log-on attempts (5) to the CLETS system disable the user's account? (FBI CJIS Security Policy 5.5.3)

    ☐ Yes ☐ No

14. Do all CLETS access devices, except for devices that are (1) part of a police vehicle; or (2) used to perform dispatch functions and located within a physically secure location, automatically lock a user out of a session after a period of inactivity? If so, what is the established time period of user inactivity before automatic session lockout? (FBI CJIS Security Policy section 5.5.5)

15. Does your agency validate and document information system accounts on an annual basis? (FBI CJIS Security Policy 5.5.1)

    ☐ Yes ☐ No

    How? Please Explain:

16. When a person with CLETS access is no longer a CLETS user **within your agency**, what is your procedure for deleting the person's CLETS access account information? (PPP 1.9.3 B)

17. When accessing CLETS **via a host interface**, what is your procedure for deleting the person's CLETS access account information?

18. Does your agency review/analyze information system audit records for indications of inappropriate or unusual activity on a weekly basis? (FBI CJIS Security Policy 5.4.3)

☐ Yes ☐ No

If no, how often?

Please Select One

19. What is your procedure if misuse is suspected?

20. Did your agency file a CLETS Misuse Investigation Reporting Form to DOJ by February 1 for the previous calendar year? (PPP 1.10.1 D.)

☐ Yes ☐ No

Please provide a copy of your agency's most recent CLETS misuse investigation reporting form.

21. If your terminal(s) with CLETS access is connected to the internet, is that access protected by a firewall or appropriate proxy server? (FBI CJIS Security Policy 5.10.1.1)

☐ Yes ☐ No ☐ N/A

If yes, please indicate:

Firewall Product Name: _____

Model/Version: _____

22. Does your agency have advanced authentication in place for devices that are not in a physically secure location? (FBI CJIS Security Policy 5.6.2.2.1)

☐ Yes ☐ No ☐ N/A

23. Does your agency have an approved system use notification message to identify the device restrictions and consent on all information systems accessing criminal justice information? (FBI CJIS Security Policy 5.5.4) Please provide a screen print of message.

☐ Yes ☐ No

24. Is the agency's encryption that is used for public, wireless, and internet network segments that transmit CLETS data protected with a least 128-bit NIST certified encryption and compliant with the NIST FIPS 140-2 requirements? (FBI CJIS Security Policy 5.10.1.2.)

☐ Yes ☐ No

25. Has your agency's SPOC reviewed and updated the network diagram? (FBI CJIS Security 5.7.1.2)

☐ Yes ☐ No

If yes, what is the last date it was reviewed and updated?

Please provide a copy.

Section 6: Record Management

1. Does your agency enter its own records into CLETS 24 hour a day?

☐ Yes ☐ No ☐ N/A Inquiry Only

If not, what agency does? _____

2. If another agency enters, do you have a Reciprocity Agreement on file? (PPP 1.5.4)

☐ Yes ☐ No ☐ N/A

Please provide a copy of the Reciprocity Agreement.

3. Does your agency respond to your own hit confirmation 24 hours a day and have access to the Master Case File at all times? (PPP 1.5.4)

☐ Yes ☐ No ☐ N/A Inquiry Only

If not, what agency does and do they have access to the Master Case File?

Is there a Time Activated Message Forwarding (TAMF) Form and Reciprocity Agreement on file?

☐ Yes ☐ No

Please provide a copy of the TAMF Form and Reciprocity Agreement.

4. Does your agency enter records into CLETS for another agency?

☐ Yes ☐ No ☐ N/A

If yes, please list or attach a list of ORI(s) and Agency name(s):

Is there a Time Activated Message Forwarding (TAMF) form and Reciprocity Agreement on file?

☐ Yes ☐ No

Please provide a copy of the TAMF and Reciprocity Agreement.

5. Does your agency perform hit confirmations for other agencies? (PPP 1.5.4)

☐ Yes ☐ No ☐ N/A

If yes, please list or attach a list of ORI(s) and Agency name(s):

Is there a Time Activated Message Forwarding (TAMF) form and Reciprocity Agreement on file?

☐ Yes ☐ No

Please provide a copy of the TAMF and Reciprocity Agreement.

If yes, does your agency access their Master Case File for hit confirmation? (NCIC 2000 Manual, Introduction 3.5)

☐ Yes ☐ No

6. 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)

☐ Yes ☐ No

Please list or attach a list of the non-subscribing agency(ies):

Is there a Release of CLETS Information Form on file? (PPP 1.5.3)

☐ Yes ☐ No

Please provide a copy of the Release of CLETS Form.

7. Has your agency placed a CLETS terminal or mnemonic with another governmental agency (i.e., family support, code enforcement, etc.)? (PPP 1.5.2)

☐ Yes ☐ No

If yes, please list or attach a list of the Agency(ies):

Is there an interagency Agreement on file? (PPP 1.5.2)

☐ Yes ☐ No

Please provide a copy of the Interagency Agreement(s).

8. Does your agency record a "third-party release" when providing Rap Sheet information, including III, to individuals outside of your agency (i.e., courts, district attorneys, probation departments, etc.)? (PPP 1.6.1 C)

☐ Yes ☐ No

9. Indicate below how your agency maintains the "third-party release" log (electronic, written, etc.)?

Please provide a sample.

10. 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

If other, please explain method of disposal:

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

Please Select One

If other, please explain method of disposal:

12. Please provide a copy of your agency's procedure for securely handling, transporting, storing and destroying media. (FBI CJIS Security Policy 5.8.3-5.8.4)

Section 7: Training (PPP 1.8.2 and NCIC 2000 Operating Manual 3.1.3)

1. Have **all** Full and Less than Full Access Operators completed the required initial training and proficiency exam within the first six months of employment?

   ☐ Yes ☐ No

2. Please explain how testing is administered and tracked.

   Submit a copy of a page from your agency's training log or NexTEST report for verification purposes.

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 IT staff, and private contractor staff? (FBI CJIS Security Policy 5.2.)

   ☐ Yes ☐ No

   Submit a copy of a page from your agency's training log, Nextest report, and/or CJIS Online (Vendors) Report for verification purposes.

4. Have all Full and Less than Full Access Operators been biennially re-certified?

   ☐ Yes ☐ No

5. Have your agency administrators read the "Areas of Liability for the Criminal Justice Information System Administrator"? (PPP 1.8.2)

   ☐ Yes ☐ No

   Submit a copy of the signature page.

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

   ☐ Yes ☐ No

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

   ☐ Yes ☐ No

   If yes, please list the methods:

Section 8: Policies and Procedures

For the following questions, if additional space is necessary please provide a copy of the procedure

1. When an information security event and/or weakness is recognized, describe your agency's procedure for reporting such security incidents (incident response plan). (CJIS Security Policy 5.3.1.)

2. Describe how your agency assigns authorization for controlling access to the information system. (CJIS Security Policy 5.5.2.)

3. Describe your agency's procedures for managing authenticators. (CJIS Security Policy 5.6.3.2.)

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

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

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

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**

For DOJ use only

The following items must be completed and documentation of such actions must be provided to DOJ within 10 days:

THIS IS NOT A COMPLETE INSPECTION UNTIL YOU RECEIVE A LETTER FROM DOJ*

As a Field Representative for the Department of Justice, I certify that:

An onsite inspection was conducted ☐
Number of fixed terminals inspected _____
Number of MDT's inspected _____
An audit was conducted via Fax or US Mail ☐

_____

(Please print) FIRST NAME LAST NAME

_____

SIGNATURE **DATE**

Notification sent to Agency on _____
Date

DOCUMENT TRANSMISSION COVER SHEET

DATE: _____ **TIME:** _____ **NO. OF PAGES:** _____ (including cover sheet)

RE: CLETS Audit

TO:

NAME: Department of Justice – Client Services
ADDRESS: PO Box 903417, Sacramento, CA 94203
OFFICE: Audits Inspections and Training
FAX NO: 916-227-2545 PHONE NO: 916-227-3332

FROM:

NAME: _____
ORI/AGENCY: _____
COUNTY: _____
ADDRESS: _____
FAX NO: _____ PHONE NO: _____

MESSAGE/INSTRUCTIONS

- ☐ Agency CLETS Coordinator (ACC) Responsibility
- ☐ Security Point of Contact (SPOC) Agreement
- ☐ CLETS Subscriber Agreement
- ☐ Private Contractor Management Control Agreement
- ☐ Samples of signed CJIS Security Addendum
- ☐ Management Control Agreement
- ☐ Terminal Location Audit
- ☐ Terminal Access Request (TAR)
- ☐ Samples of signed Employee/Volunteer Statement
- ☐ Latest Misuse Report
- ☐ Reciprocity Agreement(s)
- ☐ Time Activated Message Form (TAMF)
- ☐ Release of CLETS Form
- ☐ Interagency Agreement
- ☐ Sample of "Third-party Release" Log
- ☐ Sample of FA and LTF Training Log
- ☐ Areas of Liability for the CJIS Administrator Signature Page
- ☐ Security Awareness Training Log
- ☐ Network Diagram
- ☐ System Use Notification Message

Other Documents (Please Specify) _____