

California Department of Justice



AGENCY CLETS COORDINATOR (ACC) TRAINING

CLEARs November 2023



CLETS INSPECTIONS & DATABASE AUDITS SECTION

Field Representatives



Elisa Webb
Manager



Allison
Law



Catherine
McCain



Tara Burrows-
Yates



Melissa
Lovan



Oscar
Acosta



Michael
Frame



Sarah
Wesley



Eric
Russell

CLETS INSPECTIONS & DATABASE AUDITS SECTION

Field Representatives



Elisa Webb
Manager



Stacey Prado



DeeDee Eller



Leslie McGovern



Marisol Lopez



CLETS & CORI Transactions Compliance Section

Photo to be included

Jaimie Tackett
Manager



Danielle
Marchant



Tamara
Richardson



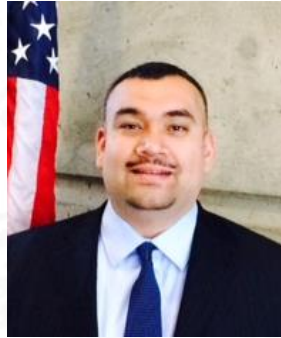
Wanda
Hoytt



DATA SHARING SECTION



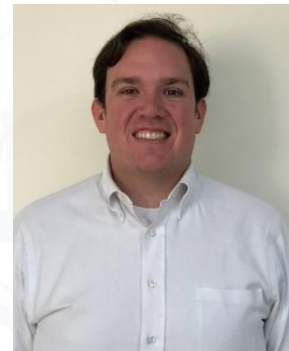
Michael Van Winkle
Manager



John Navarrete
ERDS Audits



Julie Sperr
Cal-Photo



Matthew Goude
nexTEST
CJIS Online/LASO

caldojnextest@doj.ca.gov



AGENDA



- Roles and responsibilities



- Laws/Policies/Ramifications pertaining to CLETS



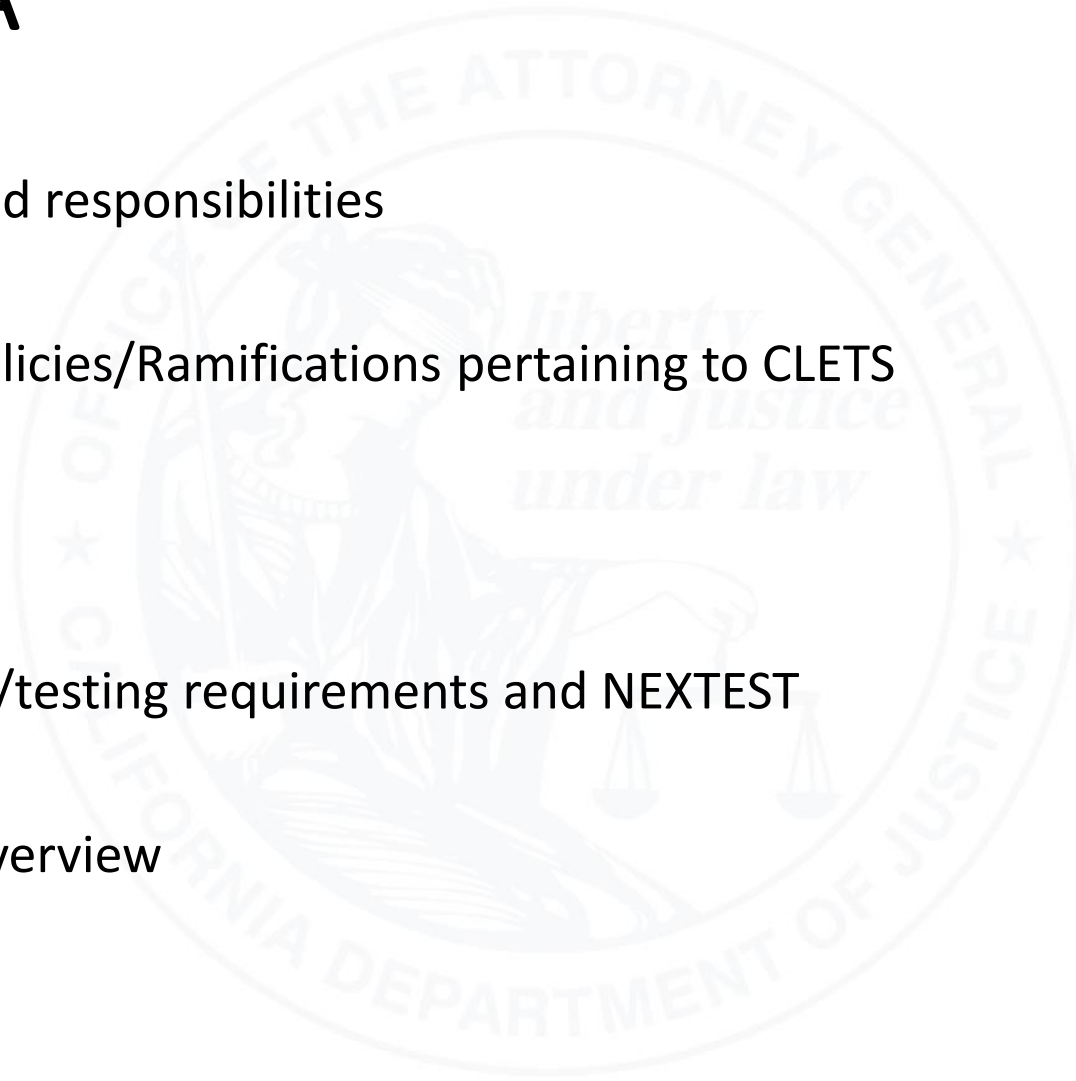
- CLEW



- Training/testing requirements and NEXTEST



- Audit Overview



ROLES AND RESPONSIBILITIES

You've been assigned as your agency's ACC...




What is an Agency CLETS Coordinator (ACC)



Ref. CLETS PPP Glossary & Section 1.3.5

SPOC – Security Point of Contact (LASO)

Rob Bonta, Attorney General

California Department of Justice CALIFORNIA JUSTICE INFORMATION SERVICES DIVISION Joe Dominic, Chief/CIO		INFORMATION BULLETIN
Subject: California Law Enforcement Telecommunications System (CLETS) New Training Requirements for Local Agency Security Officers (LASOs)	No: 22-02-CJIS Date: 03-02-2022	Contact for information: Client Services Program dojcs@doj.ca.gov

TO: ALL CRIMINAL JUSTICE AGENCIES USING THE CLETS

The purpose of this information bulletin is to provide criminal justice agencies that subscribe to CLETS guidance and resources to comply with a new requirement in the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy. Enhanced security training is now required for all Local Agency Security Officers (LASOs)¹. All criminal justice agencies authorized to access CLETS are required to appoint an LASO². The FBI's definition of LASO is interchangeable with the term "security point-of-contact" (SPOC) used in the CLETS Policies, Practices and Procedures.

NEW TRAINING REQUIREMENTS

Pursuant to prior existing federal and state requirements, LASOs were required to complete security awareness training based on their access (direct or indirect) to criminal justice information. The latest version of the FBI CJIS Security Policy expands on this requirement to mandate enhanced training annually for LASOs on the specific duties and responsibilities of those positions, and the impact on the overall security information systems:

FBI CJIS Security Policy 5.2.2

LASO training shall be required prior to assuming duties, but no later than six months after initial assignment, and annually thereafter.

At a minimum, the following topics shall be addressed as enhanced security awareness training for an LASO:

1. The roles and responsibilities listed in CJIS Security Policy Section 3.2.9.
2. Additional state/local/tribal/federal agency LASO roles and responsibilities.
3. Summary of audit findings from previous state audits of local agencies.
4. Findings from the last FBI CJIS Division audit of the CJIS Systems Agencies.
5. Most recent changes to the CJIS Security Policy.

RESOURCES TO COMPLETE THE REQUIRED TRAINING

The Department of Justice (DOJ) is offering agencies that subscribe to CLETS the new LASO training modules via its free web-based application, CJIS Online. Completion of the modules will fulfill the FBI requirements and will ensure compliance during the next CLETS audit.

¹ For reference, please refer to FBI CJIS Security Policy Appendix A8
² Required by per FBI CJIS Security Policy, Section 3.2.2.2a

communications System (CLETS): New Training Requirements for Local


acted with their CJIS Online account information, and will receive webinars.

the California Law Enforcement Web (CLEW) at

may contact DOJ's CLETS Administration Section (CAS) to update their upgrade Applications, or for other inquiries on the CLETS Policies, doj.ca.gov.

the training outlined in this bulletin, please contact DOJ's Client Services agency's assigned CLETS Audit Field Representative is also an IT contacts is available on CLEW at publications/regional-map-clets-audit_0.pdf.

Sincerely,


JOE DOMINIC, Chief/CIO
California Justice Information Services Division

For ROB BONTA
Attorney General

“The FBI's definition of LASO is interchangeable with the term "security point-of-contact" (SPOC) used in the CLETS Policies, Practices and Procedures.”

Administration/Record Keeping



Liaison with DOJ

Coordinate, maintain and submit documentation

Report misuse investigations

Every February 1st

[IB 1807-CJIS](#)



Report misuse investigations:

Every February 1st

Xavier Becerra, Attorney General

California Department of Justice CALIFORNIA JUSTICE INFORMATION SERVICES DIVISION Joe Dominic, Chief				INFORMATION BULLETIN	
Subject: California Law Enforcement Telecommunications System (CLETS) – Requirement to Report CLETS Misuse		No: 18-07-CJIS	Contact for Information: CLETS Administration Section (916) 210-4240 cas@doj.ca.gov		
		Date: 04-17-2018			

TO: ALL CALIFORNIA LAW ENFORCEMENT AGENCIES

The California Department of Justice (DOJ), in response to increasingly low submissions of misuse reporting by CLETS subscribing agencies, will be instituting changes to the reporting process to achieve 100 percent reporting of CLETS misuse. Pursuant to California Government Code section 15154 and CLETS Policies, Practices and Procedures (PPPs) section 1.10.1B, agencies that fail to report misuse annually will be subject to sanctions, up to and including, removal of CLETS service.

The DOJ considers the failure to report CLETS misuse a serious matter and will proactively enforce this requirement. CLETS PPPs section 1.10.1D prescribes that all agencies shall submit a report to the DOJ on the number of investigations performed related to the CLETS misuse, and any disciplinary action taken. Additionally, agencies are required to report whether any misuse has occurred during the reporting period. The report must be submitted by February 1 of each year, for the preceding calendar year.

Effective immediately, agencies that fail to submit the misuse report by the February 1 reporting deadline will be notified of their failure to comply and reported to the CLETS Advisory Committee (CAC) for consideration and action at the next scheduled meeting. Please note: CAC meetings are subject to the Bagley-Keene Open Meeting Act; therefore, non-reporting agencies will be posted on the California Attorney General's website and the California Law Enforcement Web (CLEW).

Misuse is defined as CLETS information that is obtained or provided outside the course of official business; a "right to know" and the "need to know" must be established. The "right to know" is defined as "authorized access to such records by statute" and the "need to know" is defined as "the information is required for the performance of official duties or functions." Other than blatant misuse, the following are examples of prohibited/unauthorized use of CLETS that include, but are not limited to:

- Querying yourself, a family member, friend, etc.;
- Providing information from the CLETS to another officer, individual, agency or company for unauthorized purposes;
- Sharing user IDs or passwords;
- Logging into CLETS and allowing others to utilize your authorized access;
- Querying the Automated Criminal History System for licensing, employment or certification purposes (e.g., Carry Concealed Weapon permits);
- Querying a firearm to determine if it is stolen prior to purchase;
- Querying the Department of Motor Vehicles to obtain unauthorized address, vehicle registration, or insurance information (e.g., querying a vehicle parked in front of your house for two days); and
- Querying high profile individuals in the media.

1 Bulletin
Requirement to Report CLETS Misuse

2

3 Misuse Investigation Reporting form (HDC 0010) is available on the CLEW website at: <http://doj.ca.gov>, or you may contact the CLETS Administration Section (CAS) to obtain a copy. Responsible for multiple Originating Agency Identifiers (ORIs) should only submit one form and list all ORIs. Forms may be e-mailed to CAS@doj.ca.gov or faxed to 916-227-0896. If you have any please contact CAS at 916-210-4240.

Sincerely,



JOE DOMINIC, Chief
California Justice Information Services Division

For XAVIER BECERRA
Attorney General

Administration/Record Keeping

Maintain user accounts

Deactivate users

- no longer employed
- delinquent on testing
- permitted access revoked

Keep up on any terminal access level changes



Administration/Record Keeping

Notify DOJ of agency information changes

- Notify DOJ's CLETS Admin Section and DOJ Field Representative
- Changes to Agency Head, ACC, SPOC, Telephone, Address



Maintain record of any contractual agreements

Example: Interagency and Reciprocity agreements

Audits/Inspections/Validations

- **Maintain mandated compliance**
State and Federal auditing requirements
- **Coordinate with DOJ for audits/inspections of your agency**
- **Coordinate and receive the validation list**
- **Prompt response to DOJ's ORI Validation Report**



Information, Publications, and Policies

Information/Publications/Policies

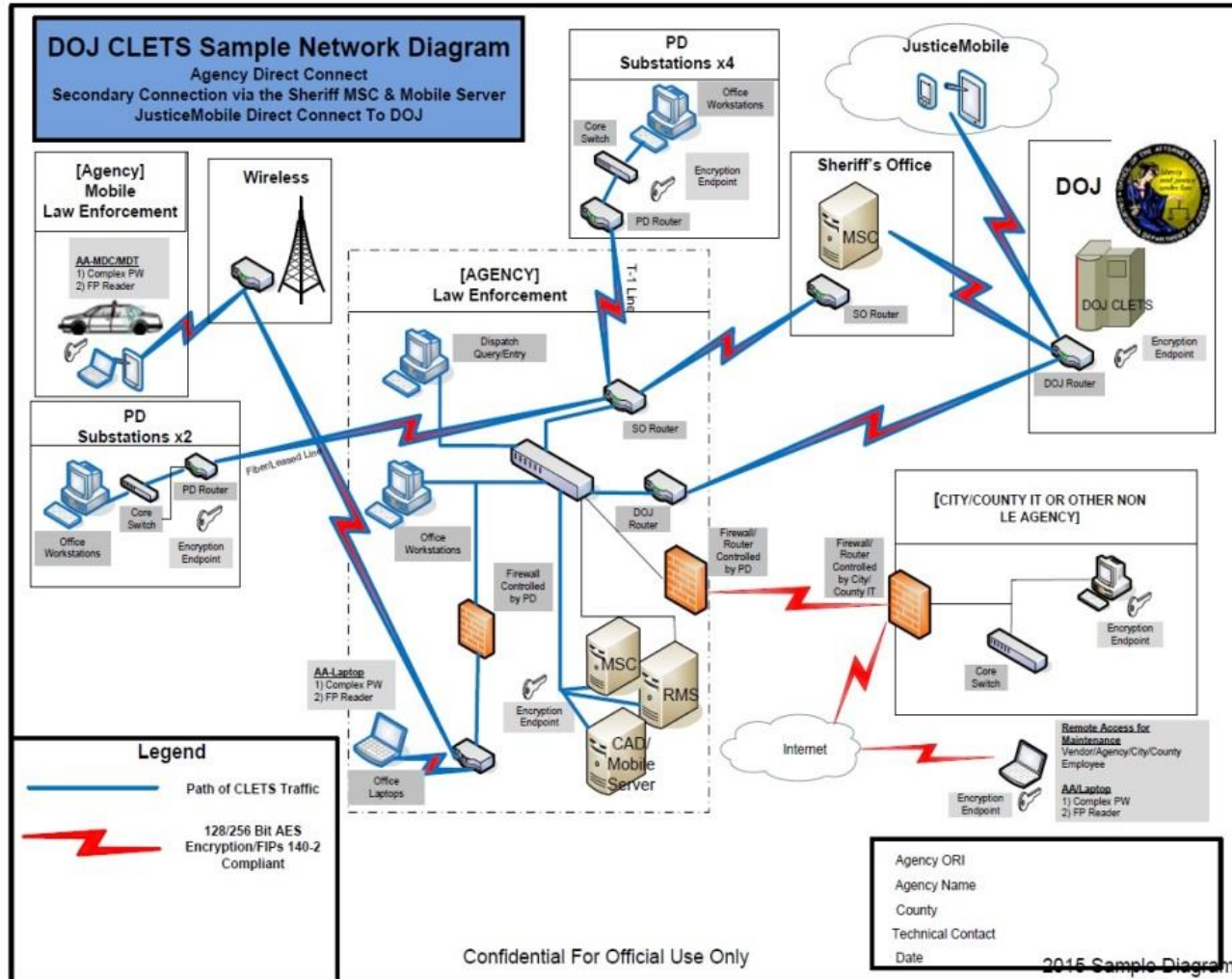
```
graph TD; A[Information/Publications/Policies] --> B[Ensure compliance with database policies and regulations]; B --> C[Ensure secure access to CLETS terminals, equipment and messages];
```

Ensure compliance with database policies and regulations

Ensure secure access to CLETS terminals, equipment and messages

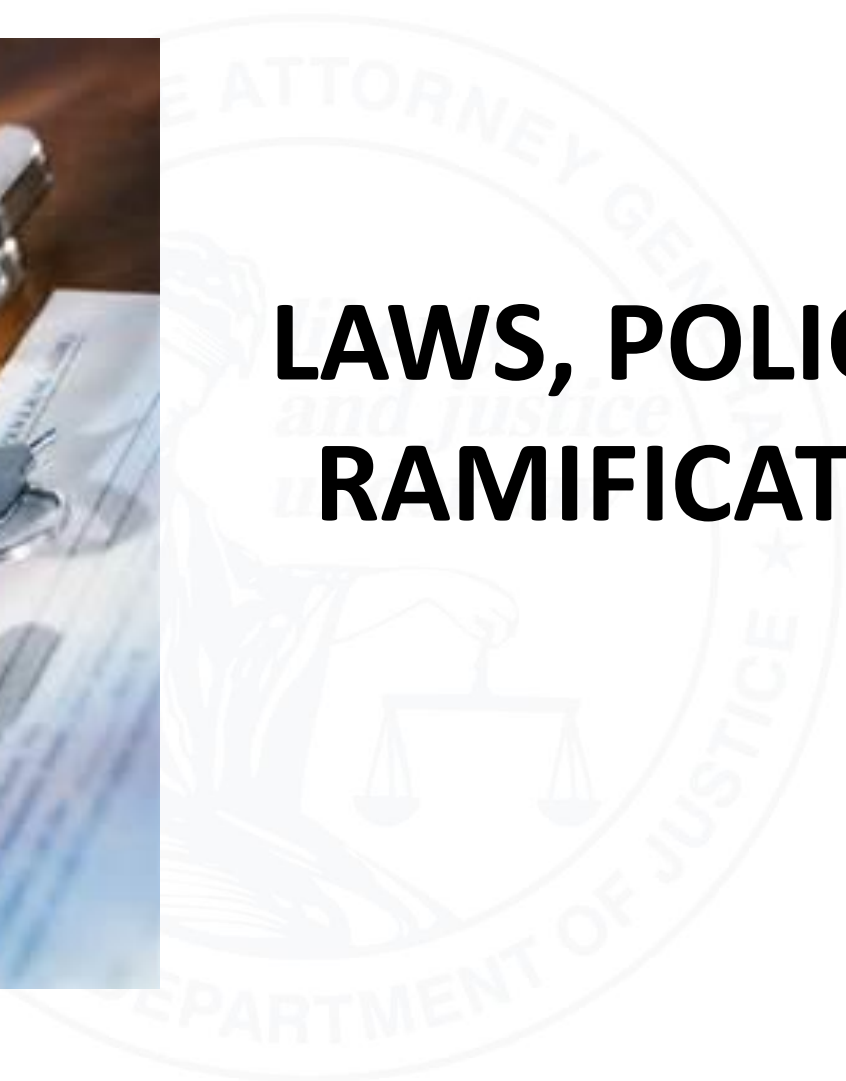
System Documentation

Maintain System Documentation and current network diagram





LAWS, POLICIES & RAMIFICATIONS



LAWS, POLICIES, & RAMIFICATIONS

The use of CLETS for other than official law enforcement purposes may result with the employing agency seeking dismissal and/or prosecution of the employee.

- PC 502
- PC 11105
- PC 11140-11143
- PC 13301-13304
- CVC 1808.45-47



LAWS, POLICIES, & RAMIFICATIONS

PC 11105

Defines who can access criminal history information

PC 11140 – 11143 - DOJ

Defines what a criminal history record is

Defines punishment for knowingly receiving and furnishing a record when not authorized

PC 13301 – 13304 - Local

Defines what a criminal history record is

Defines punishment for knowingly receiving and furnishing a record when not authorized

CVC 1808.45-1808.47

Defines willful unauthorized disclosure

Defines access by misrepresentation

Provides the penalties for violation

CLETS SECURITY

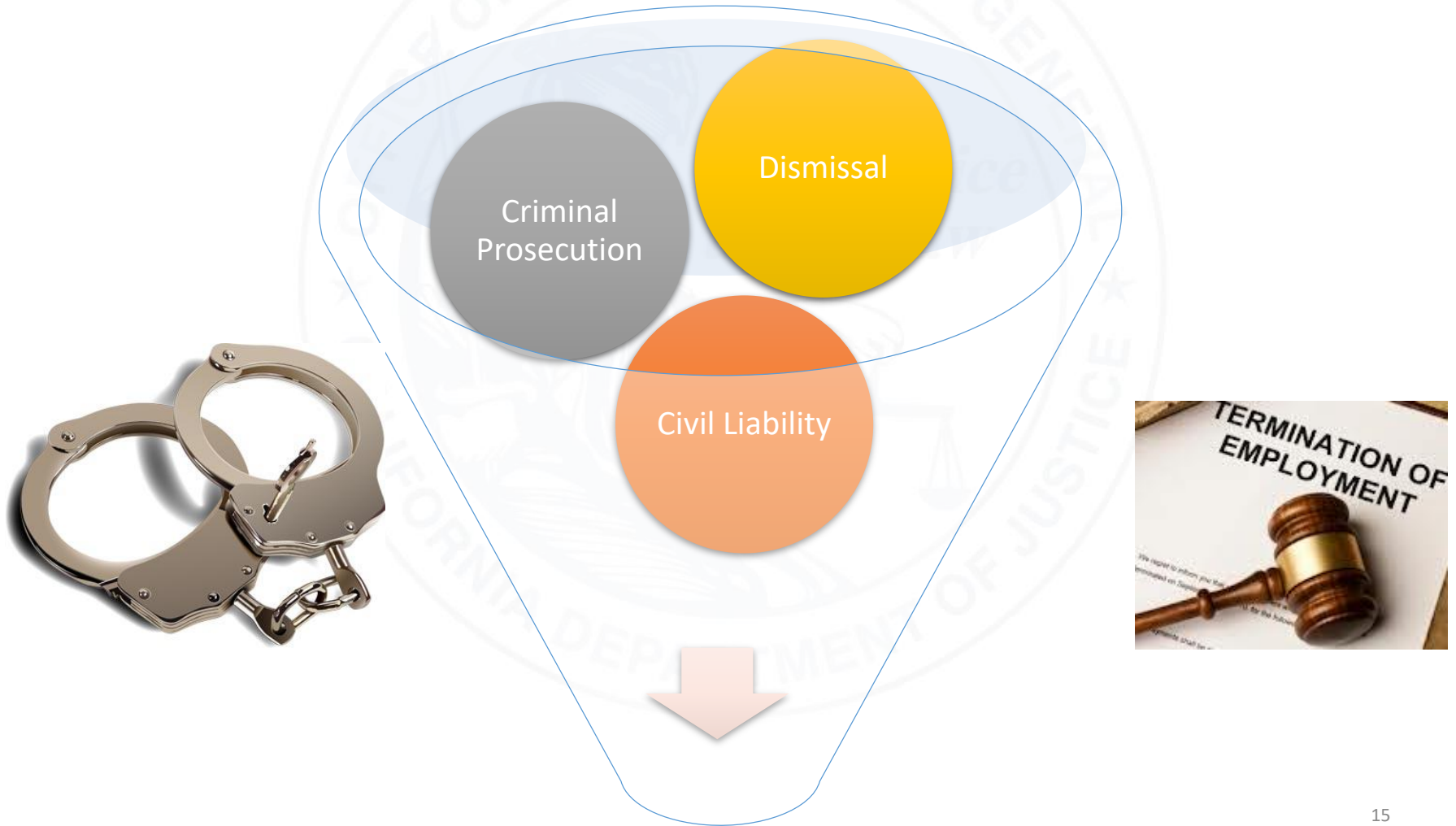


CJIS Security Policy

- Terminal security
- Terminal can not face public
- Monitors - No expectation of reasonable distance
- Remote Access
- Faxes
- Emails
- Authorized access

CLETS SECURITY

Misuse of CLETS or CLETS information may result in:



<http://www.clew.doj.ca.gov>

CLEW

CLEW Internet Access:

Any authorized employee of a Law Enforcement Agency



Search CLEW

Information Bulletin and Instructions

DOJ & BSCC Use of Force Comparison

URSUS Enrollment

URSUS Enrollment Survey

Law Enforcement Contact Process (LECP)

View LECP Submissions

OpenJustice

OpenJustice Update - Winter 2016

Citizens' Complaints Against Peace Officers - Revision

DLE-2015-06 - Information Bulletin

BCIA 724 - Revised

CJIS Programs

AB 953 - Stop Data Collection

CalGang@

CLETS

CLETS Administration Section

CLETS Application Submissions

June 1, 2022

ATTENTION

CALIFORNIA LAW ENFORCEMENT AGENCIES

Possible Legal Developments Affecting Licenses to Carry Firearms in Public Places.

March 15, 2022

ATTENTION

AGENCY CLETS COORDINATORS (ACCs) AND SECURITY POINT OF CONTACTS (SPOCs)

IMPORTANT MESSAGE REGARDING NEW TRAINING REQUIREMENTS FOR SPOCS

Beginning Wednesday, March 16, 2022, the Department of Justice (DOJ) Client Services Program is announcing the implementation of the Local Agency Security Officer (LASO) Certification module via CJIS On-Line. The LASO is synonymous with the role of the Security Point of Contact (SPOC)

FBI CJIS Security Policy Section 5.2.2 requires all LASO's to complete the certification module.

DOJ Information Bulletin 22-02-CJIS dated 03-02-2022 provides guidance for the CLETS new training requirements for LASOs.

Should you have any questions regarding this notice, please contact the Client Services Program at dojcsp@doj.ca.gov for more information. Resource information is available on CLEW at https://clew.doj.ca.gov/ccas.

January

ATTENTION

Beginn copies notific

person safety.

The Di "Califo

Should have

Client Services

Cal-Photo

CLETS Audits and Inspections Section

Client Services

Database Audits

Electronic Search Warrant Notification

(Department) will no longer send "Firearm/Ammunition" notifications will now be sent via notification to LEAs of a prohibited possession, in an effort to enhance public

in the most current version of the respective LEAs website.

Contact the Department at

The Automated Firearm System (AFS) Team is now offering beginner and advanced user training. To request a training, visit the training request form.

ATTENTION: APPS/FDAS USERS

In order to view/download the APPS and/or FDAS Secure Mailbox report(s), you must submit an APPS/FDAS Report(s) Request along with a signed authorization form (BOF 054) from the head of agency or his/her designee for review and approval.

Pursuant to Penal Code section 30000, the information contained in the Prohibited Armed Persons File (also known as the Armed Prohibited Persons System) is confidential. The Department of Justice may only release that information through the California Law Enforcement Telecommunications System to those entities specified in subdivisions (b) or (c) of Section 11105 and only for the purpose of determining if a person is armed and prohibited from possessing firearms. Any information you receive from the Department under this authority may not be shared outside of your law enforcement agency. The information is exempt from disclosure in response to a Public Records Act request.

Download BOF 054 Form

APPS/FDAS Report(s) Request

ANNUAL CLETS MISUSE REPORTING

Submit CLETS Misuse Investigation Report

Manage Submitted Reports



INCIDENT RESPONSE PLAN (IRP)



What is an IRP? (CJIS Security Policy 5.3)

A formal written plan outlining an agency's security incident response protocol

Defines when the CLETS IT Security Incident Response form would be used

TRAINING



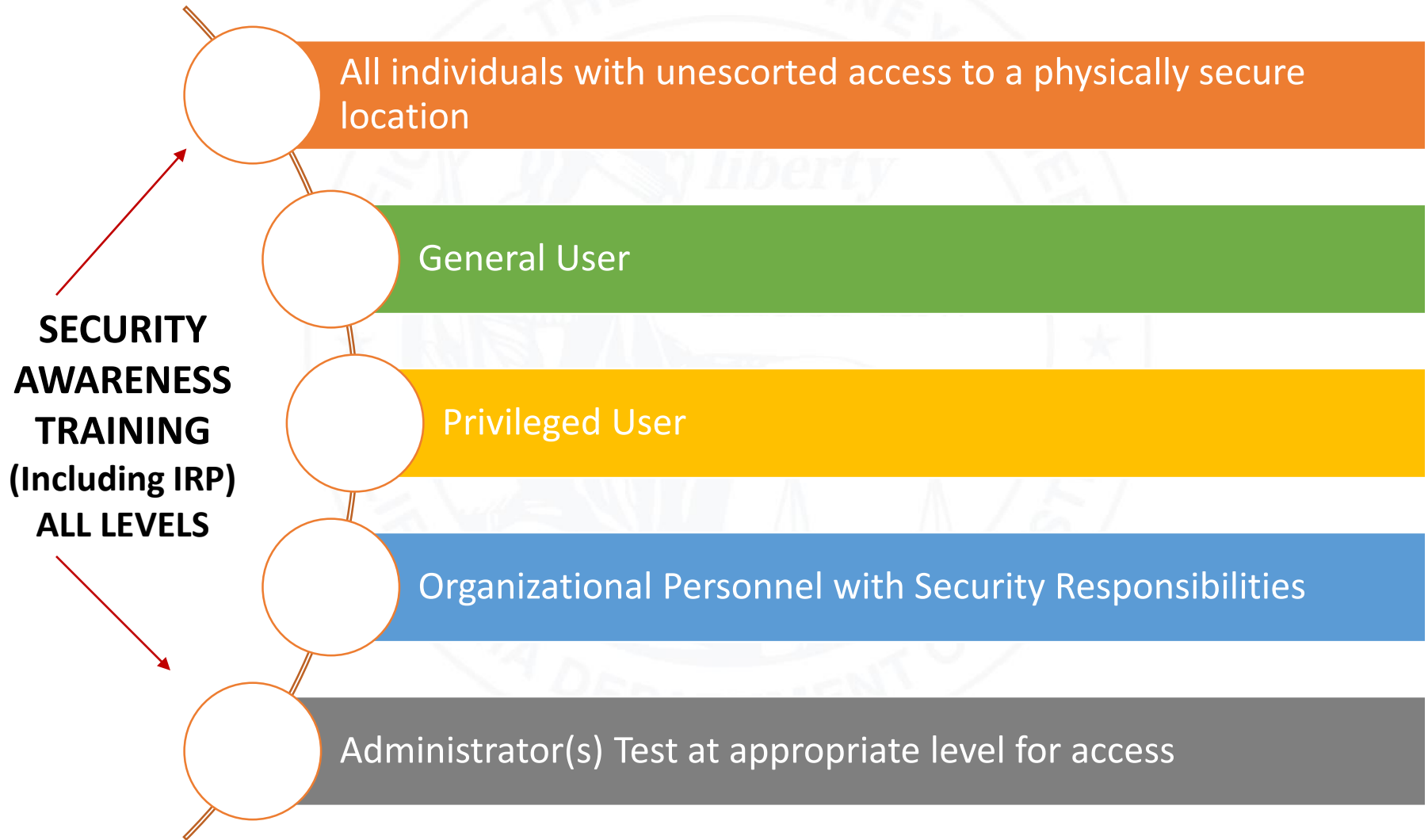
TRAINER EXPECTATIONS

Provide new employees with overview of CLETS/CLETS databases

Be current on state laws and policies related to CLETS/CLETS information

Have the resources available to track CLETS training for your agency

ROLE-BASED TRAINING

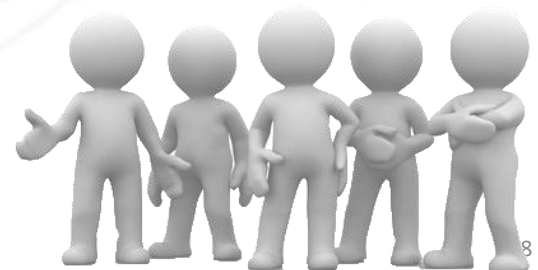


All individuals with unescorted access to a physically secure location

ref. CLETS PPP 1.6.4, CLETS PPP 1.8.3, and CJIS Security Policy 5.2 AT-3

**Any individual who is unescorted in a physically secure location
and can hear/see CLETS derived information**

Physically Secure Location is defined as a facility, a criminal justice conveyance, or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.



Security Awareness

Unescorted Access Example

A local police department hires custodial staff that will have physical access throughout the PD (a physically secure location) after normal business hours to clean the facility.

These personnel have unescorted access to a physically secure location and therefore must be given the awareness training on all the topics identified in **CJISSECPOL AT-3 d 1**.

General User

ref. CLETS PPP 1.6.4, CLETS PPP 1.8.3, and CJIS Security Policy 5.2 AT-3

A user, but not a process, who is authorized to use an information system

Information System is defined as a system of people, data, and processes, whether manual or automated, established for the purpose of managing information.



General User

Awareness and Training

A Sheriff's Office has employed a number of dispatchers. As part of their daily duties, the dispatchers run CJI queries by request from the Sheriff and deputies.

The dispatchers access CJI both logically (running queries) and physically (printed copies of reports containing CJI).

The dispatchers have direct access to CJI and are required to complete the awareness training on all the topics identified in **CJISSECPOL AT-3 d 1 and 2.**

Privileged User

ref. CLETS PPP 1.6.4 and CLETS PPP 1.8.3 and CJIS Security Policy 5.2 AT-3

A user authorized (and, therefore, trusted) to perform security relevant functions that general users are not authorized to perform



Privileged User

Awareness and Training Example

The State Police hired system and network administrator personnel to bolster the security of the state network.

Some duties may include creating accounts for new personnel, implementing security patches for existing systems, creating backups of existing systems, and implementing access controls throughout the network.

The system and network administrators have privileged access to CJI/CJI-processing systems and are required to complete the awareness training on all the topics identified in **CJISSECPOL AT-3 d 1, 2, and 3.**

Organizational Personnel with Security Responsibilities

ref. CLETS PPP 1.6.4 and CLETS PPP 1.8.3 and CJIS Security Policy 5.2 AT-3

Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJJ and the implementation of technology in a manner compliant with the CJISSECPOL



Organizational Personnel with Security Responsibilities

Personnel responsible to ensure the confidentiality, integrity, CJI availability, and implementation of technology in a manner compliant with the CJISSECPOL Section 5.2 AT-3 (d) (1), (2), and (3).

Including the following topics:

- Local Agency Security Officer Role (LASO)
- Authorized Recipient Security Officer Role (ARSO)
- Additional state/local/tribal/territorial or federal agency roles and responsibilities
- Summary of State and FBI audit findings



ADMINISTRATOR and UPPER LEVEL MANAGEMENT

ref. CLETS PPP 1.8.2 A1-A7

An Administrator is not exempt from role based training.

Appropriate training is based on individual access, security/privacy requirements, and assigned duties.

Required Training:

- Administrator(s) must review and sign the NCIC's "Areas of Liability for the Criminal Justice Information System Administrator"
- Shall test at appropriate level for access granted.

NEXTEST

Format for adding accounts to NexTEST

Reports

Initial training module

NexTEST vs CJIS online

Expired Users – NexTEST Expiration Report



AUDITS



Database Audits

- Focuses on the integrity of the data and compliance with the CJIS and NCIC requirements (records)

CORI Audit

- Identify compliance & non-compliance as it pertains to the “need to know & right to know” including the “route to” field (RTE) and III.

CLETS Audit

- Centers on physical, administrative and technical security processes and well as, reviews policies, physical terminal security, testing.

CORI AUDIT

CORI Pre-Audit

CORI On-Site
Audit

III Audit
(Purpose Codes)



CORI AUDITS

Pre-Audit questionnaire



California Department of Justice
Criminal Offender Record Information (CORI)
Pre-Audit Questionnaire



Agency _____	County _____	Date _____
Person Completing Audit _____	Title _____	Telephone Number _____
Mailing Address _____	Email Address _____	Fax Number _____
Head of Agency _____	Email Address _____	Telephone Number _____

1. Please list your agency's ORI(s) and provide a list of your agency's California Law Enforcement Telecommunications System (CLETS) terminals; identifying mnemonics (MNE), and physical street address. An automated printed list can be attached.
2. Does your agency have access to the NCIC Interstate Identification Index (III)?
 Yes No
3. Does your agency make inquiries into the Automated Criminal History System (ACHS) and/or NCIC Interstate Identification Index (III) for other agencies?
ACHS Yes No III Yes No
If yes, list agencies.
4. How does your agency maintain an audit trail for CORI and III inquiries?

CORI AUDITS



Most Common Errors:

Lack of
documentation

Route to Field
not compliant

Missing case
number

CORI AUDITS

Two Part Compliance:

- Right to know *and* Need to know
- Route to field

Route to field requirements:

- Requester
- User(if different)
- Specific reason for inquiry
 - *Case number is best*

THIRD PARTY RELEASE LOGS

The log must be maintained when CORI and/or III is furnished to an outside agency.

The log must contain:

- Name of Requestor
- Requesting Agency
- Date
- What Info was Given
- How the Info was Transmitted
- The log must be available for inspection for a minimum of three years

CA Code of Regulations - Title 11 Division 1 Chapter 7 Article 1 subsection 707 (c)

DATABASE AUDITS

Full
Access
agencies
only

Agency notified of Audit Selection (30 days prior)

Pre-audit questionnaire sent to the agency

Random selection of database records (approx. 50)

On Site Audit conducted and Preliminary Audit Finding Report issued at the end of the audit

Final Audit Report sent to Agency Head within 30-60 days after the audit.

DATABASE AUDITS



Most Common Errors:

No second
party checks

Records not
updated

Consultations
not
completed

DATABASE AUDITS

Audited Databases:

Automated Boat System (ABS)

Automated Firearms System (AFS)

Automated Property Systems (APS)

California Restraining and Protective
Order System (CARPOS)

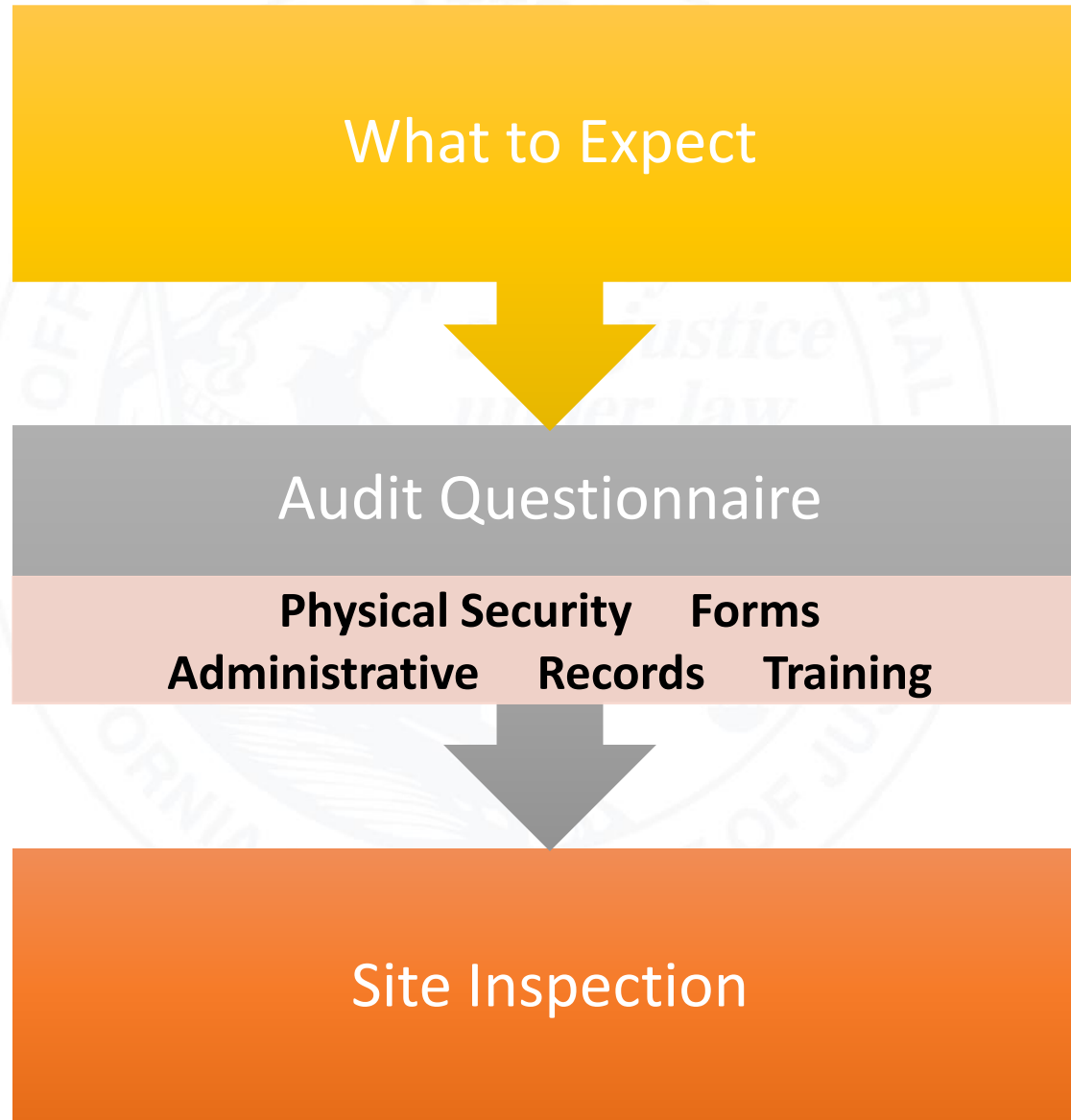
California Sex and Arson Registry
(CSAR)

Missing Persons System (MPS)

Stolen Vehicle System (SVS)

Wanted Person System (WPS)

CLETS AUDITS



CLETS AUDITS

Most Common Errors:

Terminals
accessible
to the
public

Trustees in
accessible
areas

Missing
forms or
forms not
updated

Expired
users

Training
records not
maintained
or updated

RESOURCES



Know your resources:

Are policy/training manuals readily accessible?

Know your DOJ contacts

NCIC

FBI CJIS

PPP

DOJ Field Reps assigned to your agency

Activity (Chat)

For each of the following pictures

Assume all computers can access CLETS

Assume all windows are public

Assume all counters are public







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)

Please Select One:

Sometimes

Always

Rarely

Never

CLETS INSPECTIONS & DATABASE AUDITS SECTION

Contact information:

DOJCSP@doj.ca.gov



Oscar Acosta



Eric Russell