CA Law Enforcement Telecommunications System

T4T UPDATE

CLEARS November 2023

CLETS INSPECTIONS & DATABASE AUDITS SECTION

Field Representatives

Elisa Webb
Manager

Allison
Law

Catherine
McCoin

Melissa
Lovan

Eric
Russell

Oscar
Acosta

Michael
Frame

Sarah
Wesley

Tara
Burrows-Yates

CLETS Audit Field Representative Assignment Map

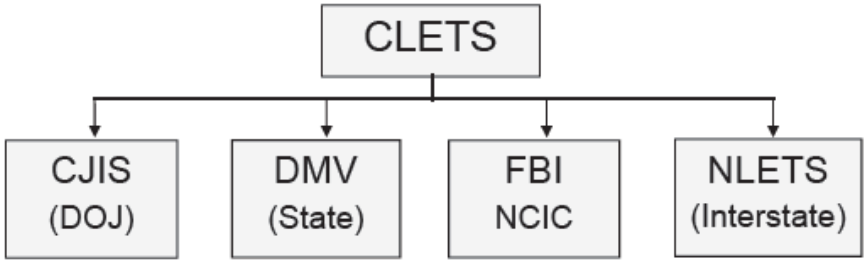
DOJCSP@doj.ca.gov

PURPOSE & AGENDA

This training provides trainers with the updates on resources, materials and requirements regarding initial training.

AGENDA

- Introduction
- Review
  - Expectations and Responsibility of a trainer
  - Changes in Levels of Training
  - Initial Training requirements
  - Approved formats for Initial Training
  - Local Agency Security Officer (LASO)



CJIS (DOJ)

Armed & Prohibited Persons – System
Automated Archive System
Automated Boat System
Automated Criminal History - System
Automated Firearms System
Automated Property System
CA Restraining & Protective - Order System
CA Sex & Arson Registry
Criminal History System
Manual Criminal History
Mental Health Firearm - Prohibition System
Name and Number Inquiry
Missing & Unidentified Persons - System
Stolen Vehicle System
Supervised Release File
Wanted Persons System

DMV (State)

Driver License/Identification - Card
International Registration Plan
Occupational Licensing
Parking/Toll Violation
Vehicle/Vessel Registration File

FBI/NCIC

Article File
Boat File
Foreign Fugitive File*
Gang File*
Gun File
Identity Theft File*
Image File
Immigration Violator File
Interstate Identification - Index*
Known or Appropriately - Suspected Terrorist File*
License Plate File
Missing Persons File
National Sex Offender - Registry
NICS Denied Transaction – File*
ORI File
Protection Order File
Protective Interest File*
Securities File*
Supervised Release File
Unidentified Persons File
Vehicle File
Vehicle/Boat Parts File
Violent Person File
Wanted Persons File

NLETS (Interstate)

Administrative Messages
Canadian Police Information - Centre
Commercial Vehicle – Information*
Concealed Weapons - Information*
Criminal History
Driver's License/Driver History
FAA Aircraft Registration*
Hazardous Material File*
Help Files*
Fixed Format Hit Confirmation
INTERPOL*
Law Enforcement Support – Center*
National Center for Missing and - Exploited Children*
National Insurance Crime Bureau
ORION File*
Parole/Probation/Corrections*
Sex Offender Registration*
Vehicle/Boat/Snowmobile - Registration
Wildlife Violation File

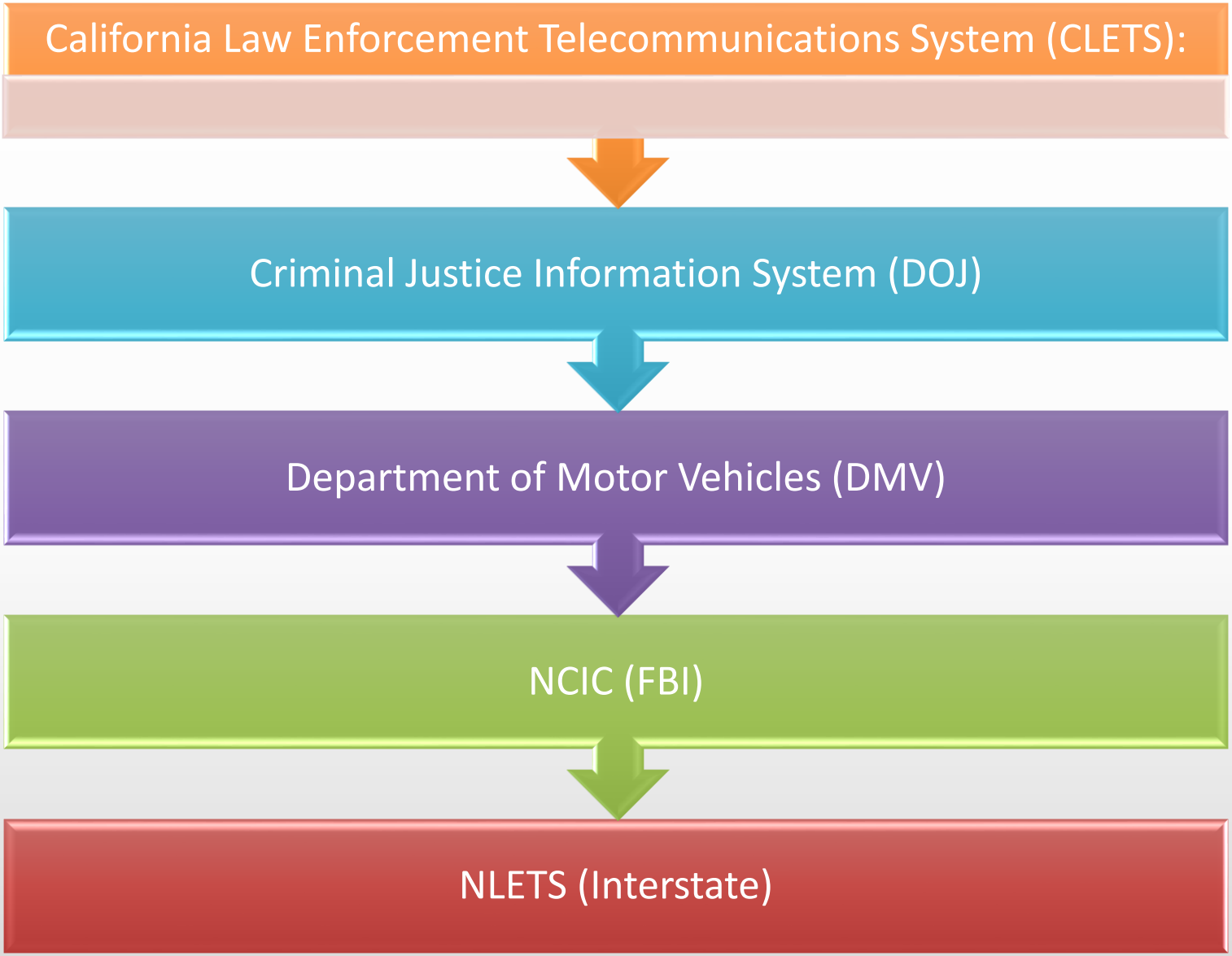
CLETS can be accessed through:
Message Switching Computer
CAD/LAN/WAN – Interfaces
LEAWEB – Direct Connect

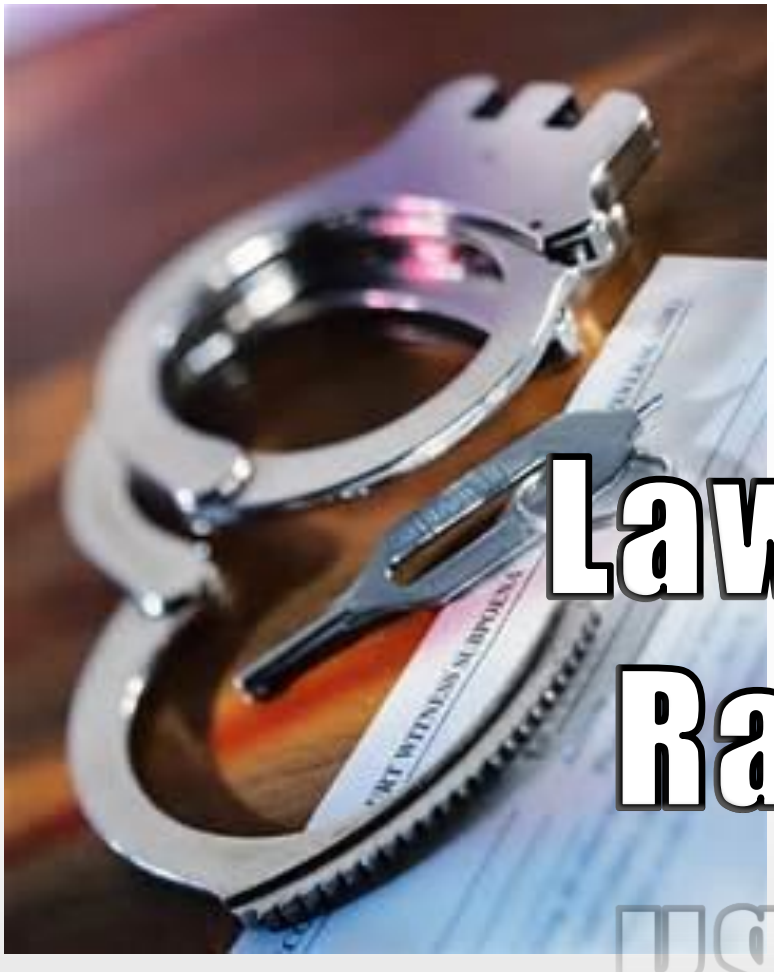
****NOTE****

Oregon LEDS is no longer available via the CLETS. Inquires intended for LEDS will need to be performed through the International Justice and Public Safety Network using the National Law Enforcement Telecommunications System (NLETS).

*Non-Corollary Files and Systems

Ref. guide inside cover


California Law Enforcement Telecommunications System (CLETS):
Criminal Justice Information System (DOJ)
Department of Motor Vehicles (DMV)
NCIC (FBI)
NLETS (Interstate)



Laws, Policies & Ramifications

LAWS, POLICIES & RAMIFICATIONS

LAWS

- Penal Codes
- CA Code of Regulations
- Other Statutes

POLICIES

- CLETS Policies, Practices & Procedures
- FBI CJIS Security Policy
- NCIC Operating Manual

RAMIFICATIONS

- Dismissal
- Criminal Prosecution
- Civil Liability

Laws, Policies & Ramifications

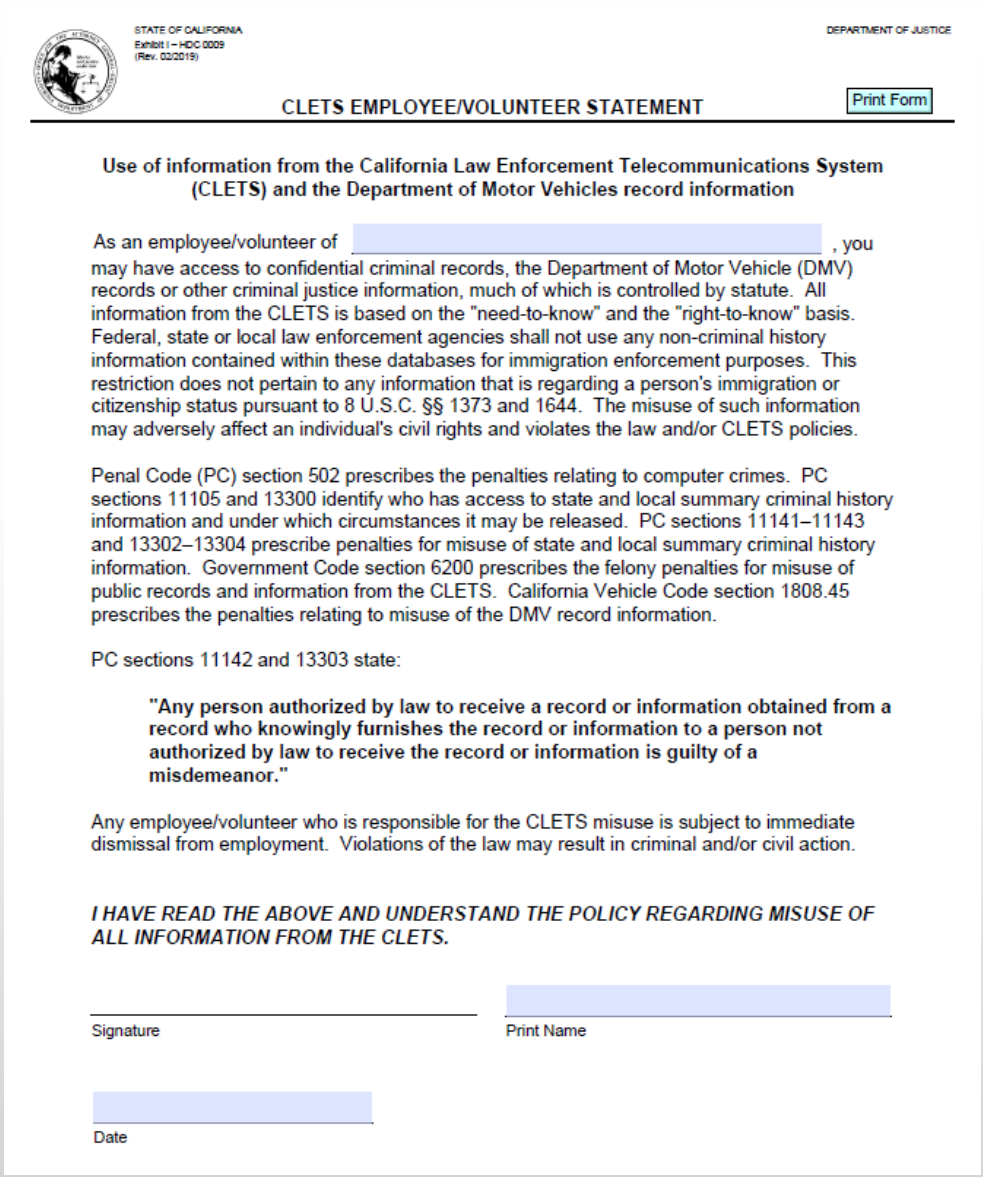
The use of CLETS for other than official law enforcement purposes may result with the employing agency seeking dismissal and/or prosecution of the employee

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

CLETS SECURITY

- Employee Volunteer Statement
- Remote Access
- Emails

Employee Volunteer Statement



STATE OF CALIFORNIA
Exhibit I – HDC 0009
(Rev. 02/2019)

DEPARTMENT OF JUSTICE

CLETS EMPLOYEE/VOLUNTEER STATEMENT

Print Form

Use of information from the California Law Enforcement Telecommunications System (CLETS) and the Department of Motor Vehicles record information

As an employee/volunteer of _____ , you may have access to confidential criminal records, the Department of Motor Vehicle (DMV) records or other criminal justice information, much of which is controlled by statute. All information from the CLETS is based on the "need-to-know" and the "right-to-know" basis. Federal, state or local law enforcement agencies shall not use any non-criminal history information contained within these databases for immigration enforcement purposes. This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to 8 U.S.C. §§ 1373 and 1644. The misuse of such information may adversely affect an individual's civil rights and violates the law and/or CLETS policies.

Penal Code (PC) section 502 prescribes the penalties relating to computer crimes. PC sections 11105 and 13300 identify who has access to state and local summary criminal history information and under which circumstances it may be released. PC sections 11141–11143 and 13302–13304 prescribe penalties for misuse of state and local summary criminal history information. Government Code section 6200 prescribes the felony penalties for misuse of public records and information from the CLETS. California Vehicle Code section 1808.45 prescribes the penalties relating to misuse of the DMV record information.

PC sections 11142 and 13303 state:

> **"Any person authorized by law to receive a record or information obtained from a record who knowingly furnishes the record or information to a person not authorized by law to receive the record or information is guilty of a misdemeanor."**

Any employee/volunteer who is responsible for the CLETS misuse is subject to immediate dismissal from employment. Violations of the law may result in criminal and/or civil action.

I HAVE READ THE ABOVE AND UNDERSTAND THE POLICY REGARDING MISUSE OF ALL INFORMATION FROM THE CLETS.

_____ _____

Signature Print Name

_____

Date

System Use Notification Message

THIS SYSTEM IS RESTRICTED TO AUTHORIZED USERS FOR LEGITIMATE LAW ENFORCEMENT PURPOSES. THE INFORMATION CONTAINED IN THIS SYSTEM MEETS THE DEFINITION OF CRIMINAL OFFENDER RECORD INFORMATION (PENAL CODE SECTION 11075). THIS INFORMATION IS CONFIDENTIAL AND SHALL BE ACCESSED ONLY IN THE PERFORMANCE OF OFFICIAL DUTIES. YOUR USAGE OF THIS SYSTEM IS AUDITED AND MONITORED. UNAUTHORIZED ACCESS, ACCESS FOR OTHER THAN OFFICIAL PURPOSES, OR DISSEMINATION TO UNAUTHORIZED PERSONS IS UNLAWFUL AND MAY RESULT IN ADMINISTRATIVE, CIVIL, OR CRIMINAL SANCTIONS. MODIFICATION OF THIS SYSTEM OR THE DATA CONTAINED THEREIN OR IN TRANSIT TO/FROM, IS PROHIBITED BY LAW AND MAY BE REPORTED TO LAW ENFORCEMENT BY SYSTEM PERSONNEL. THE INFORMATION DISPLAYED BY THIS SYSTEM MAY NOT CONTAIN ALL ENTRIES FOR A SUBJECT'S RECORD. TO OBTAIN COMPLETE RECORD INFORMATION, REFER TO THE SYSTEM OF RECORD.

LEAWEB

Username

Password

Remember Me

Sign In

FBI CJIS Security Policy

5.5.4 System Use Notification

The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules.

The system use notification message shall, at a minimum, provide the following information:

- 1. The user is accessing a restricted information system.
- 2. System usage may be monitored, recorded, and subject to audit.
- 3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
- 4. Use of the system indicates consent to monitoring and recording.

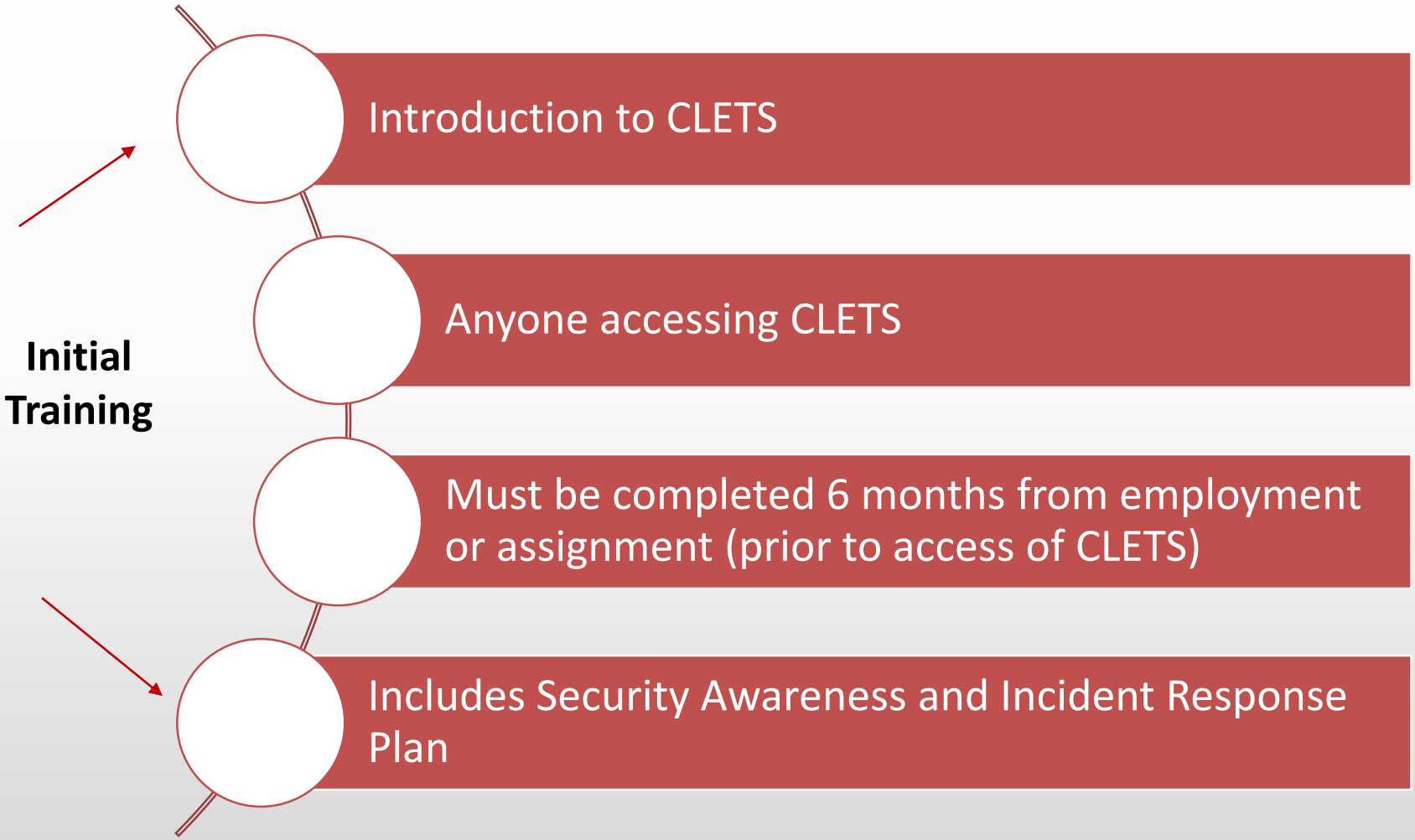
CLETS SECURITY

Misuse of CLETS or CLETS provided information may result in:

- Dismissal
- Criminal Prosecution
- Civil Liability

INITIAL TRAINING

INITIAL TRAINING



DOJ CERTIFIED TRAINERS

- Instructors must be DOJ certified
- Academy instruction if approved by DOJ
- DOJ certification does not expire
- Initial Training Materials approved by DOJ
- nexTEST module ≠ DOJ certified trainer

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

Formats for Initial Training

No time or length of training requirement

Academy Trainers/Training

Agency created

on-line training

Agency led instruction

CJIS

On-Line

nexTEST

INCIDENT RESPONSE PLAN (IRP)

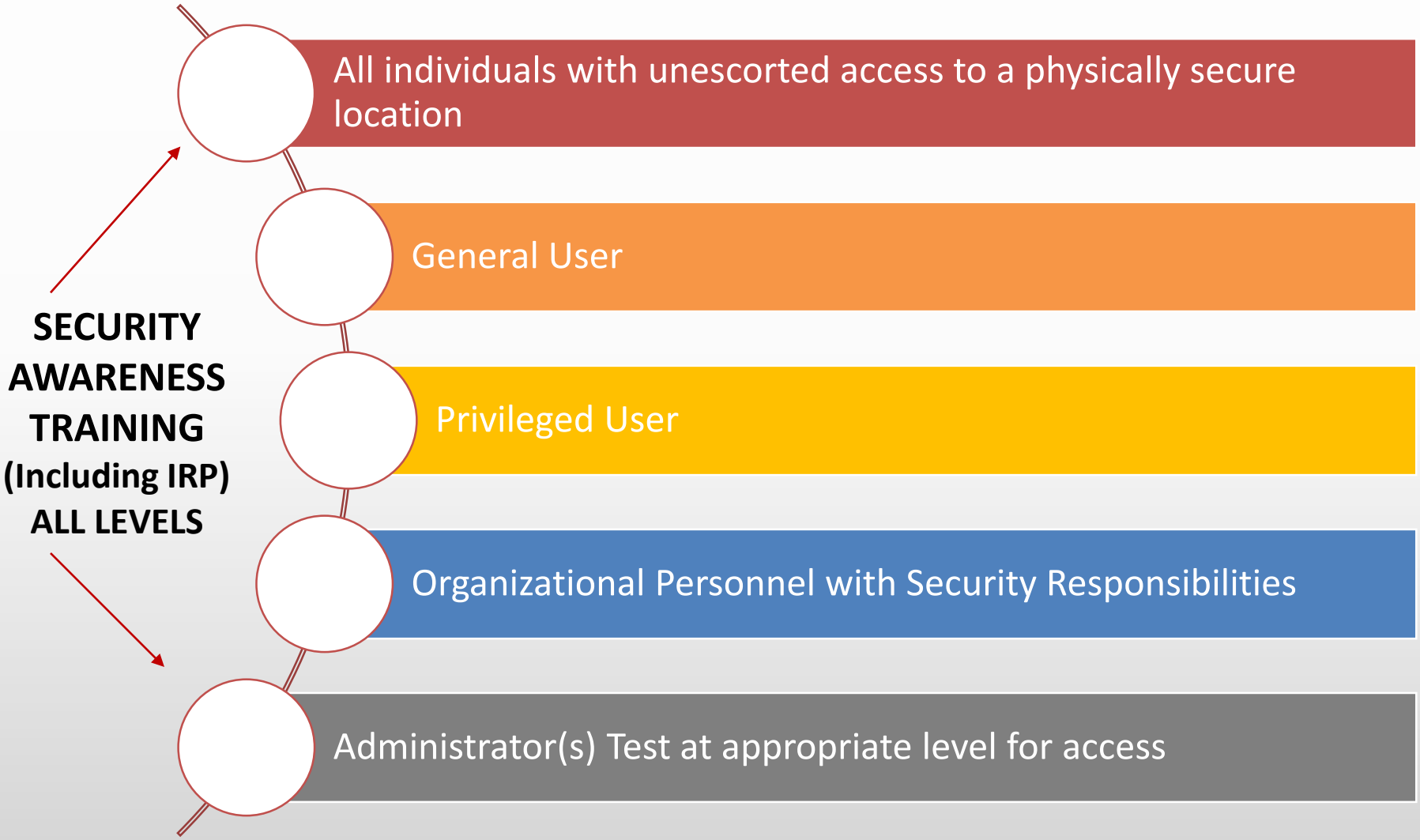
FBI CJIS Security Policy Section 5.3

- A formal written plan outlining an agency's security incident response protocol
- Defines when the CLETS IT Security Incident Response form would be used

Security Awareness Training

All users with authorized access to CJI should be made aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI.

ROLE-BASED TRAINING

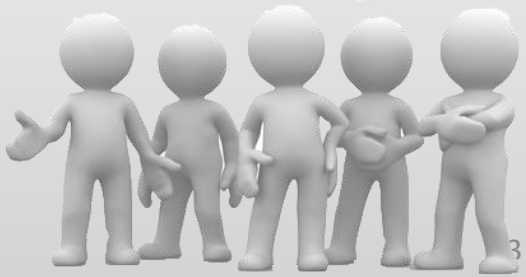


All individuals with unescorted access to a physically secure location

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 CJI 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 CAL/PHOTO CONTACTS

Email:

caldojnextest@doj.ca.gov

Julie Sperr
Cal-Photo

Matthew Goude
NexTEST/CJIS Online

Michael Van Winkle, Manager

LOCAL AGENCY SECURITY OFFICER (LASO)

FBI CJIS SECURITY POLICY 5.2.2

Federal and State requirements states LASO's are required to complete security awareness training based on their access (direct or indirect) to criminal justice information. (ie. General, Privileged)

In addition, the current FBI CJIS Security Policy mandates enhanced security awareness for all LASOs.

LASO ENHANCED TRAINING

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 a LASO:

- The roles and responsibilities listed in CJIS Security Policy Section 3.2.9.
- State/local/tribal/federal agency LASO roles and responsibilities.
- Summary of audit findings from previous FBI CJIS Audit.
- IB 22-02-CJIS


Q&A

DOJ CLETS INSPECTION & DATABASE AUDIT SECTION

THANKS FOR ATTENDING

Contact information: DOJCSP@doj.ca.gov

Oscar Acosta

Eric Russell