California Department of Justice **Office of General Counsel** **Information Security Office** **Lloyd Indig, Chief Information Security Officer,** **CJIS Systems Agency Information Security Officer**		**INFORMATION BULLETIN**

Information Bulletin: 2026-ISRS-001

Subject: U. S. Department of Justice Federal Bureau of Investigation Criminal Justice Information Services Division Criminal Justice Information Services (CJIS) Security Policy, Version 6.1 (June 26, 2026)

Date: July 24, 2026

Contacts: California Department of Justice (DOJ) Information Security Office
(916) 210-2879
cadoj@doj.ca.gov

DOJ's California Law Enforcement Telecommunications System Administration Section
(916) 210-4240
cas@doj.ca.gov

* * * *

TO: ALL CLETS SUBSCRIBING AGENCIES

This information bulletin provides all agencies that subscribe to the California Law Enforcement Telecommunication System (CLETS) highlights of recent changes to the U. S. Department of Justice, Federal Bureau of Investigation (FBI), Criminal Justice Information Services Division, Criminal Justice Information Services (CJIS) Security Policy (CJISSECPOL or FBI CJIS Security Policy).

FBI CJIS Security Policy version 6.1

Effective June 26, 2026, the FBI released version 6.1 of the FBI CJIS Security Policy, which includes changes previously approved by the FBI CJIS Advisory Policy Board (APB). In addition, the FBI released the Requirements Companion Document to the FBI CJIS Security Policy, version 6.1.

The current FBI CJIS Security Policy and the FBI Requirements Companion Document can be found at: https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center [1].

Summary of CJISSECPOL Version 6.1 APB Approved Changes

[1] If the current link changes in the future and you have difficultly locating the operative one, please contact the DOJ Information Security Office at cadojiso@doj.ca.gov.

1. Addressing Omissions, Corrections, and Additions to the Modernized *CJIS Security Policy* (*CJISSECPOL*) Part 1, Spring 2025, APB#16, SA#1: update sections with approved changes.
2. Addressing Omissions, Corrections, and Additions to the Modernized *CJIS Security Policy* (*CJISSECPOL*) Part 2, Spring 2025, APB#16, SA#2: update sections with approved changes.
3. Addressing Omissions, Corrections, and Additions to the Modernized *CJIS Security Policy* (*CJISSECPOL*) Part 3, Spring 2025, APB#16, SA#3: update sections with approved changes.

Administrative Changes

1. Administrative Changes approved by the Security and Access Subcommittee on November 14, 2025

Note: Administrative changes are vetted through the Security and Access Subcommittee and not the entire APB process.

Key to APB approved changes (e.g., "Modernizing Personnel Security (PS) in the *CJISSECPOL*, Spring 2024, APB#11, SA#7: modernize the CJIS Security Policy requirements for:")

Topic Paper Title
Spring 2024 - Advisory Policy Board cycle and year
APB# - Advisory Policy Board Topic number
SA# - Security and Access Subcommittee Topic number Summary of change

The approved APB changes to the FBI CJIS Security Policy made by version 6.1 are as follows:

- In all "dash"-1(b) requirements, standardize on designating "organizational personnel" with "information security" responsibilities and not just "security" responsibilities. This applies to the AC, IA, IR, MA, MP, and RA control families.
  - Designate ~~an individual~~ **organizational personnel** with **information** security responsibilities to manage the development, documentation, and dissemination of the incident response policy and procedures; and
- Throughout the CJISSECPOL, the phrase "process, store, or transmit" is used to describe system component containing CJI.
  - CM-12(b): Identify and document the users who have access to ~~the system.~~**CJI** and system components where ~~the information~~ **CJI** is **processed, stored, or transmitted** ~~processed and stored~~; and
  - CM-12(c): Document changes to the location (i.e., system or system components) where ~~the information~~ **CJI** is **processed, stored, or transmitted** ~~processed and stored~~.
  - RA-2(a): Categorize the system and information it processes, stores, **or** ~~and~~ transmits;
  - MA-6: Obtain maintenance support and/or spare parts for critical system components that process, store, **or** ~~and~~ transmit CJI within agency-defined recovery time and recovery point objectives of failure.

- Appendix G.1 Virtualization: This appendix documents security considerations for implementing and operating virtual environments that process, store, ~~and/~~ or transmit Criminal Justice Information.

- Pre-modernized physical security requirements were germane to a physically secure location as defined in Appendix A. Modernized Physical and Environmental Protection (PE) controls did not include the physically secure location designation.
  - **Physical and environmental protection policy and procedures address the controls in the PE family that are implemented within organizations for protection of physically secure locations which are 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**

- Addresses concerns about controlling egress from facilities and physically secure locations.
  - PE-3 a. Enforce physical access authorizations by:
    1. Verifying individual access authorizations before granting access to the facility; and
    2. Controlling ingress ~~and egress~~ to the facility using agency-implemented procedures and controls;

- The Alternate Work Site control, PE-17, requires encryption of CJI both at-rest and in-transit.
  - PE-17 b. Employ the following controls at alternate work sites:
    4. Follow the encryption requirements found in SC-13 and SC-28 for electronic storage (i.e., **data in-transit** and data at-rest) of CJI.

- The topics required for Awareness Training (AT) are now directly linked to actual controls in the CJISSECPOL.
  - AT-~~3~~ (d)(1) All individuals with unescorted access to a physically secure location
    - ~~a. Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information Penalties~~
    - ~~b. Reporting Security Events~~
    - ~~c. Incident Response Training~~
    - ~~d. System Use Notification~~
    - ~~e. Physical Access Authorizations~~
    - ~~f. Physical Access Control~~
    - ~~g. Monitoring Physical Access~~
    - ~~h. Visitor Control~~
    - ~~i. Personnel Sanctions~~
    - **a. Section 4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information**

Penalties

c. IR-2 Incident Response Training

d. IR-6 Incident Reporting

e. PE-2 Physical Access Authorizations

f. PE-3 Physical Access Control

g. PE-6 Monitoring Physical Access

h. PE-8 Visitor Access Records

i. PS-8 Personnel Sanctions

- AT-3 (d)(2)General User: A user, but not a process, who is authorized to use an information system.

~~a. Criminal Justice Information~~

~~b. Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information~~

~~c. Personally Identifiable Information~~

~~d. Information Handling~~

~~e. Media Storage~~

~~f. Media Access~~

~~g. Audit Monitoring, Analysis, and Reporting~~

~~h. Access Enforcement~~

~~i. Least Privilege~~

~~j. System Access Control~~

~~k. Access Control Criteria~~

~~l. System Use Notification~~

~~m. Session Lock~~

~~n. Personally Owned Information Systems~~

~~o. Password~~

~~p. Access Control for Display Medium~~

~~q. Encryption~~

~~r. Malicious Code Protection~~

~~s. Spam and Spyware Protection~~

~~t. Cellular Devices~~

~~u. Mobile Device Management~~

~~v. Wireless Device Risk Mitigations~~

~~w. Wireless Device Malicious Code Protection~~

~~x. Literacy Training and Awareness/Social Engineering and Mining~~

~~y. Identification and Authentication (Organizational Users)~~

~~z. Media Protection~~

a. Section 4.1 Criminal Justice Information

b. Section 4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information

c. Section 4.3 Personally Identifiable Information

d. AC-3 Access Enforcement

e. AC-6 Least Privilege

f. AC-8 System Use Notification

g. AC-11 Device Lock

h. AC-18 Wireless

i. AC-20 Use of External Systems

j. AT-2(3) Literacy Training and Awareness/Social Engineering and Mining

k. AU-6 Audit Record Review, Analysis and Reporting

l. CA-3 Information Exchange

m. IA-2 Identification and Authentication (Organizational Users)

n. IA-5(1)(a) Memorized Secret Authenticators and Verifiers

o. MP Media Protection

p. MP-2 Media Access

- AT-3 (d)(3) Privileged User: A user that is authorized (and, therefore, trusted) to perform security relevant functions that general users are not authorized to perform.

~~a. Access Control~~

~~b. System and Communications Protection and Information Integrity~~

~~c. Patch Management~~

~~d. Data backup and storage—centralized or decentralized approach~~

~~e. Most recent changes to the CJIS Security Policy~~

a. AC Access Control

b. CP-6 Alternate Storage Site

c. CP-9 System Backup

d. SC System and Communications Protection

e. SI-2 Flaw Remediation

f. Most recent changes to the CJIS Security Policy

- AT-3 (d)(4) Organizational Personnel with Security Responsibilities: 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.

  a. Section 3.2.9 Organizational Personnel with Security Responsibilities ~~Local Agency Security Officer Role~~

- AT-3: In version 5.9.2 and earlier of the CJISSECPOL, the CJIS Systems Officer (CSO)/State Identification Bureau (SIB) Chief had the latitude to accept awareness training from other agencies. That latitude was not carried into the modernized AT controls.

  NOTE: The CSO/SIB Chief may accept the documentation of the completion of role-based security and privacy training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

- AT-2: The term "incident" is used throughout the CJISSECPOL to describe occurrences of unauthorized actions or access involving CJI.

  - (a)(2): When required by system changes or within 30 days of any security **incident** ~~event~~ for individuals involved in the **incident** ~~event~~;

- As the CJISSECPOL was modernized, many cross-references were created. Since the various control families were approved at different times, discrepancies were created in several of the cross-references based on changes made throughout the APB process.

  - IA-5(1)(b)(3) If look-up secrets are distributed online, then they SHALL be distributed over a secure channel in accordance with the post-enrollment binding requirements in IA-5**(n)(16)** ~~'n' 17~~ through **(22)** ~~25~~.

  - IA-5(1)(c)(20) If out-of-band verification is to be made using the PSTN, then changing the pre-registered telephone number is considered to be the binding of a new authenticator and SHALL only occur as described in IA-5**(n)(16)** ~~n (17)~~ through **(22)** ~~(25)~~.

  - IA-5(o)(1)(j) Secrets used for session binding SHALL time out and not be accepted after the times specified in IA-5**(j)(10) and IA-5(j)(11)** ~~j (13)~~ as appropriate for the AAL.

  - When incidents or suspected incidents occur, notification is key to the incident handling process. Notification should happen immediately, not after confirmation.

    - IR-6(b): Report incident information to organizational personnel with incident handling

responsibilities, ~~and if confirmed~~, notify the CSO, SIB Chief, or Interface Agency Official, **and FBI CJIS ISO**.

- Inaccuracies existed in the MP-6 control. Language is specific to digital media but is written such that it would apply to non-digital media as well. Additionally, there are methods used as examples that are not practical for a certain type of media.
  - MP-6(a): Sanitize or destroy digital ~~and non-digital~~ media prior to disposal, release out of agency control, or release for reuse using overwrite technology at least three times or ~~degauss~~ **degaussing** ~~digital media prior to disposal or release for reuse by unauthorized individuals.~~ Inoperable digital media will be destroyed (cut up, shredded, etc.). ~~Physical~~ **Non-digital** media will be securely disposed of when no longer needed for investigative or security purposes, whichever is later. ~~Physical~~ **Non-digital** media will be destroyed by crosscut shredding or incineration; and
- Two requirements under AAL2 are only applicable to federal government agencies.
  - IA-5(j)(6) Verifiers operated by **federal** government agencies at AAL2 SHALL be validated to meet the requirements of FIPS 140 Level 1.
  - IA-5(j)(7) Authenticators procured by **federal** government agencies SHALL be validated to meet the requirements of FIPS 140 Level 1.
- Encryption is a prime protector of criminal justice information (CJI) when outside a physically secure location.
  - SC-13(b): Implement the following types of cryptography required for each specified cryptographic use: cryptographic modules which are Federal Information Processing Standard (FIPS) 140-3 certified, or **a** FIPS validated algorithm for symmetric key encryption and decryption (FIPS 197 [AES]), with a symmetric cipher key of at least **256-bit** ~~128-bit~~ strength for CJI in transit.
  - SC-28: Protect the confidentiality and integrity of the following information at rest: CJI when outside physically secure locations using cryptographic modules which are certified FIPS 140-3 with a symmetric cipher key of at least **256-bit** ~~128-bit~~ strength, or FIPS 197 with a symmetric cipher key of at least 256-bit strength.
- SI-2(2) Flaw Remediation | Automated Flaw Remediation Status and RA-5 Vulnerability Monitoring and Scanning both relate to a vulnerability scan of the information system.
  - SI-2(2): Determine if system components have applicable security-relevant software and firmware updates installed using vulnerability scanning tools at least **monthly** ~~quarterly~~ or following any security incidents involving CJI or systems used to process, store, or transmit CJI.
  - RA-5: Monitor and scan for vulnerabilities in the system and hosted applications at least monthly and when new vulnerabilities potentially affecting the system are identified and reported;

Under the CLETS Policies, Practices, and Procedures (PPP), all agencies with CLETS access must adhere to the requirements established in the PPP and the FBI CJISSECPOL. Further, each agency is responsible for annually reviewing the requirements of the PPP and FBI CJISSECPOL to ensure the agency is still in compliance.

The FBI CJISSECPOL contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of CJI. The FBI CJISSECPOL imposes appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. It also provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. The FBI CJISSECPOL applies to every individual, contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity, with access to, or who operates in support of, criminal justice services and CJI.

Agencies are encouraged to conduct a comprehensive review of the FBI CJISSECPOL and the Requirements Companion Document to identify the areas that may require changes to technical systems or implementation of new administrative controls.

* * * *

For information security questions relating to requirements of the FBI CJISSECPOL, please contact the DOJ Information Security Office at cadojiso@doj.ca.gov. For CLETS or PPP questions, please contact the CLETS Administration Section at (916) 210-4240 or cas@doj.ca.gov.

Sincerely,

Lloyd Indig

LLOYD INDIG
Chief Information Security Officer,
CJIS Systems Agency Information Security Officer

For ROB BONTA
Attorney General