


<p>California Department of Justice Office of General Counsel Information Security &amp; Research Services</p> <p>Lloyd Indig, Chief Information Security Officer</p>		<p><b>INFORMATION BULLETIN</b></p>
---	--	--

Information Bulletin: 2025-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 6.0 (December 27, 2024)

Date: February 1, 2025

Contacts: CA DOJ Information Security Office  
[cadoj@doj.ca.gov](mailto:cadoj@doj.ca.gov)

CLETS Administration Section  
(916) 210-4240  
[cas@doj.ca.gov](mailto: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 Criminal Justice Information Services Division Criminal Justice Information Services (CJIS) Security Policy (CJISSECPOL).

FBI CJISSECPOL 6.0

Effective December 27, 2024, the FBI released version 6.0 of the FBI CJISSECPOL, 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 CJISSECPOL, version 6.0.

Effective in version 6.0 contains modernized control families of Assessment, Authorization, & Monitoring, Personnel Security, System and Services Acquisition, and Supply Chain Risk Management. As a reminder, Priority One controls are those controls that must be implemented immediately as analysis shows that these controls considerably improve your security posture against known active attacks. Priorities Two, Three, and Four can be considered a roadmap for implementation in that order. FBI CJIS audit of version 6.0 will start on October 1, 2025.

The approved APB changes to the FBI CJISSECPOL, version 6.0 are as follows:

- Modernizing the Executive Summary, Section 1: Introduction, Section 2: CJISSECPOL Approach, and Section 3: Roles and Responsibilities in the CJISSECPOL, Spring 2024, APB#11, SA#2: update sections with approved changes.
- Changing and Refreshing Authenticators in the CJISSECPOL, Spring 2024, APB#11, SA#3: clarifies which authenticator type requires annual changing and clarifies the use of a “banned password” list.
- Modernizing System and Services Acquisition (SA) in the CJISSECPOL, Spring 2024, APB#11, SA#5: add definitions and modernize the CJIS Security Policy requirements for:

- System and Services Acquisition Policy and Procedures Allocation of Resources
- System Development Lifecycle Acquisition Process
- System Documentation
- Security and Privacy Engineering Principles External System Services
- Developer Configuration Management Developer Testing and Evaluation Developer Process, Standards, and Tools
- Modernizing Supply Chain and Risk Management (SR) in the CJISSECPOL, Spring 2024, APB#11, SA#6: modernize the CJIS Security Policy requirements for:
  - Supply Chain Risk Management Policy and Procedures Supply Chain Risk Management Plan
  - Acquisition Strategies, Tools, and Methods Notification Agreements
  - Inspection of Systems or Components Component Disposal
- Modernizing Personnel Security (PS) in the CJISSECPOL, Spring 2024, APB#11, SA#7: modernize the CJIS Security Policy requirements for:
  - Personnel Security Policy and Procedures Position Risk Designation
  - Personnel Screening Personnel Termination Personnel Transfer Access Agreements
  - External Personnel Security
  - Personnel Sanctions Position Descriptions
- Modernizing Assessment, Authorization, and Monitoring (CA) in the CJISSECPOL, Spring 2024, APB#11, SA#8: modernize the CJIS Security Policy requirements for:
  - Assessment, Authorization, and Monitoring Policy and Procedures Control Assessments
  - Information Exchange
  - Plan of Action and Milestones Authorization
  - Continuous Monitoring Internal System Connections
- Remove Appendix J and K from the CJISSECPOL, Spring 2024, APB#11, SA#9: remove the indicated appendices.

The current FBI CJISSECPOL and the FBI Requirements Companion Document can be found at: <https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center><sup>1</sup>.

Under the CLETS Policies, Practices, and Procedures (PPP) section 1.3.2, 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 CJ. The FBI CJISSECPOL imposes appropriate controls to protect the full lifecycle of CJ, whether at rest or in transit. It also provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJ. 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 CJ.

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.

---

<sup>1</sup>If the current link changes in the future and you have difficulty locating the operative one, please contact the CA DOJ Information Security Office at [cadojiso@doj.ca.gov](mailto:cadojiso@doj.ca.gov).

\* \* \* \*

For information security questions relating to requirements of the FBI CJISSECPOL, please contact the CA DOJ Information Security Office at [cadojiso@doj.ca.gov](mailto:cadojiso@doj.ca.gov).

For CLETS or PPP questions, please contact the CLETS Administration Section at (916) 210-4240 or [cas@doj.ca.gov](mailto:cas@doj.ca.gov).

Sincerely,

*Lloyd Indig*

LLOYD INDIG  
Chief Information Security Officer

For ROB BONTA  
Attorney General