


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

Information Bulletin: 2024-ISRS-002
Subject: (FBI) Criminal Justice Information Services (CJIS) Security Policy, Version 5.9.5 (July 9, 2024)
Date: August 9, 2024

Contacts: DOJ Information Security Office
cadoj@doj.ca.gov

CLETS 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 Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (CJISSECPOL).

FBI CJISSECPOL 5.9.5

Effective July 9, 2024, the FBI released version 5.9.5 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 5.9.5.

Effective in version 5.9.5, priority and implementation markings have been added to the modernized controls. Based on the FBI Director approved APB recommendation, beginning October 1, 2024, requirements existing prior to the CJISSECPOL modernization (i.e., version 5.9) and those identified as Priority 1 will be the set of sanctionable requirements. Non-modernized sections do not have markings but are considered “existing” requirements and continue to be auditable and sanctionable. All Priority 2, Priority 3, and Priority 4 modernized requirements fall into a zero-cycle status. The zero-cycle begins October 1, 2024, and ends September 30, 2027.

Starting October 1, 2024, and aligning with the APB decision, the CJIS Security Policy Information Technology Security Audit team will be auditing Priority 1 controls and controls that existed in version 5.9 dated June 1, 2020.

Note: A “zero-cycle” is understood to mean that entities will have one audit cycle from the CJISSECPOL Information Technology Security Audit team of review and educate but not sanction. One audit cycle equals 3 years due to the triennial audit requirement of CSAs in section 5.11 Policy Area 11: Formal Audits of the CJISSECPOL. If an entity is audited in fiscal year 2025 by the CJISSECPOL Information Technology Security Audit team, all priority 2 - 4 controls will not be sanctioned (and most likely not audited) until the fiscal year 2028 audit.

You will find a prioritized list of all the modernized controls in the CJISSECPOL and Requirements Companion Document. Both the FBI and DOJ recommend that you implement Priority 1 controls immediately to improve your security posture against known active attacks. Priorities Two, Three, and Four (indicated by P2, P3, and P4 in the CJISSECPOL and Companion Document) are considered a roadmap for implementation in that order.

The approved changes to the FBI CJISSECPOL, version 5.9.5 are as follows:

- Section 5.6 Identification and Authentication, IA-5(1)a Authenticator Management | Authenticator Types, Memorized Secret Authenticators and Verifiers, Fall 2023, APB#15, SA#1, Create a Sunset Date for “Basic Password Standards” in the CJISSECPOL
- Section 5 Policy and Implementation, Fall 2023, APB#15, SA#2, CJISSECPOL Security Control Priority and Implementation Deadlines
- Section 5.7 Configuration Management, Fall 2023, APB#15, SA#3, Modernizing Configuration Management (CM) in the CJISSECPOL

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 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

For ROB BONTA
Attorney General