


<p>California Department of Justice Office of General Counsel Information Security & Research Services Lloyd Indig, Chief Information Security Officer</p>		<p>INFORMATION BULLETIN</p>
<p><i>Subject:</i></p>	<p><i>No.</i> 2024-ISRS-001</p>	<p><i>Contact for information:</i> DOJ Information Security Office cadojiso@doj.ca.gov CLETS Administration Section (916) 210-4240 cas@doj.ca.gov</p>
<p>Federal Bureau of Investigation Criminal Justice Information Services Security Policy Security Requirements</p>	<p><i>Date:</i> 03/15/2024</p>	

TO: ALL CLETS SUBSCRIBING AGENCIES

This information bulletin provides criminal justice agencies that subscribe to the California Law Enforcement Telecommunication System (CLETS) with a reminder about mandatory implementation of multi-factor authentication, in accordance with the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy. This bulletin also highlights recent changes to the FBI CJIS Security Policy.

Multi-factor Authentication

Agencies should be aware of the FBI CJIS Security Policy requirements governing access to Criminal Justice Information (CJI), including mandatory implementation of multi-factor authentication (MFA) for privileged and non-privileged accounts. The MFA requirement will be sanctionable for audit by the FBI starting October 1, 2024. (See FBI CJIS Security Policy § 5.6 Identification and Authentication.)

FBI CJIS Security Policy 5.9.4

Effective December 20, 2023, the FBI released version 5.9.4 of the FBI CJIS Security Policy, which includes changes previously approved by the FBI CJIS Advisory Policy Board. A number of these items are currently in effect and auditable, and some changes will be sanctionable for audit by the FBI starting October 1, 2024. The changes made in FBI CJIS Security Policy 5.9.4 are as follows:

- Section 5.4 Audit and Accountability: Modernizes the FBI CJIS Security Policy requirements for Audit and Accountability Policy and Procedures, Event Logging, Content of Audit Records, Audit Log Storage Capacity, Response to Audit Logging Process Failures, Audit Record Review, Analysis and Reporting, Audit Record Reduction and Report Generation, Time Stamps, Protection of Audit Information, Audit Record Retention, and Audit Record Generation.
- Section 5.9 Physical and Environmental Protection: Modernizes the FBI CJIS Security Policy requirements for Physical and Environmental Policy and Procedures, Physical Access

Authorizations, Physical Access Control, Access Control for Transmission, Access Control for Output Devices, Monitoring Physical Access, Visitor Access Records, Power and Equipment Cabling, Emergency Shutoff, Emergency Power, Emergency Lighting, Fire Protection, Environmental Controls, Water Damage Protection, Delivery and Removal, and Alternate Work Site.

- Section 5.10 System and Communications Protection: Modernizes the FBI CJIS Security Policy requirements for Systems and Communications Protection Policy and Procedures, Separation of System and User Functionality, Information in Shared System Resources, Denial-of-Service Protection, Boundary Protection, Transmission Confidentiality and Integrity, Network Disconnect, Cryptographic Key Establishment and Management, Cryptographic Protection, Collaborative Computing Devices and Applications, Public Key Infrastructure Certificates, Mobile Code, Secure Name/Address Resolution Service (Authoritative Source), Secure Name/Address Resolution Service (Recursive or Caching Resolver), Architecture and Provisioning for Name/Address Resolution Service, Session Authenticity, Protection of Information At Rest, and Process Isolation.
- Section 5.17 Planning: Modernizes the FBI CJIS Security Policy requirements for Planning Policy and Procedures, System Security and Privacy Plans, Rules of Behavior, Security and Privacy Architectures, Central Management, Baseline Selection, and Baseline Tailoring.
- Section 5.18 Contingency Planning: Modernizes the FBI CJIS Security Policy requirements for Contingency Planning Policy and Procedures, Contingency Plan, Contingency Training, Contingency Plan Testing, Alternate Storage Site, Alternate Processing Site, Telecommunications Services, System Backup, and System Recovery and Reconstitution.
- Section 5.19 Risk Assessment: Modernizes the FBI CJIS Security Policy requirements for Risk Assessment Policy and Procedures, Security Categorization, Risk Assessment, Vulnerability Monitoring and Scanning, Risk Response, and Criticality Analysis.
- Appendix D Sample Information Exchange Agreements: Revision to the CJIS Systems User Agreement

FBI CJIS Security Policy 5.9.3

As a reminder, notable changes made by FBI CJIS Security Policy 5.9.3 include:

- Section 5.3 Incident Response: Modernizes the FBI CJIS Security Policy requirements for Incident Response Policy and Procedures, Incident Response Training, Incident Response Testing, Incident Handling, Incident Monitoring, Incident Reporting, Incident Response Assistance, and Incident Response Plan.
- Section 5.5 Access Control: Modernizes the FBI CJIS Security Policy requirements for Access Control Policy and Procedures, Account Management, Access Enforcement, Information Flow Enforcement, Separation of Duties, Least Privilege, Unsuccessful Logon Attempts, System Use Notification, Device Lock, Session Termination, Remote Access, Wireless Access, Access Control for Mobile Devices, Use of External Systems, Information Sharing, and Publicly Accessible Content.
- Section 5.16 Maintenance: Modernizes the FBI CJIS Security Policy requirements for Maintenance Policy and Procedures, Controlled Maintenance, Maintenance Tools, Nonlocal Maintenance, Maintenance Personnel, and Timely Maintenance.

Compliance with CLETS and FBI CJIS Security Policy Requirements

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 CJIS Security Policy. Further, each agency is responsible for annually reviewing the requirements of the PPP and FBI CJIS Security Policy to ensure the agency is still in compliance.

The FBI CJIS Security Policy 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 CJIS Security Policy 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 CJIS Security Policy applies to every individual, contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity, with access to, or who operate in support of, criminal justice services and CJ.

Agencies are encouraged to conduct a comprehensive review of the FBI CJIS Security Policy 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 CJIS Security Policy, 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
Office of General Counsel
Information Security & Research Services

For ROB BONTA
Attorney General