



Important Update:

2024 FBI CJIS Security Policy Release v. 5.9.5



August 2024

Newsletter: 2024 - 00004

Executive Summary:

The Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) has released version 5.9.5 of the CJIS Security Policy (CJISSECPOL). Please share with your LASO and IT Personnel.

On July 9, 2024, the FBI released version 5.9.5 of the CJIS Security Policy (CJISSECPOL). The updated policy and related Requirements Companion document are posted on CJIS Security Policy Resource Page and Omnixx Links under the IT Assistance Link. This updated version includes a modernized Configuration Management (CM) control family, a sunset date for the "Basic Password Standards", and CJISSECPOL Security Control Priority and Implementation Deadlines.

Below is a summary of the changes that were implemented:

5.7 Configuration Management (CM)

The Configuration Management (CM) family of controls establish requirements like those previously in Section 5.7 of the CJISSECPOL. Many of the existing requirements were carried over. However, there are new controls which address aspects of managing the configuration of the information system not previously considered in the CJISSECPOL. This updated control family includes new controls for creating a system baseline configuration, maintaining previous versions of baseline configurations to support rollback, establishing a configuration change process, and maintaining a system component inventory.

Important Information for:

Criminal Justice Agencies, Non-Criminal Justice Agencies, Executives/Administrators, Local Agency Security Officers (LASO), Terminal Agency Coordinators (TAC), and technical support staff.

Sunset of "Basic Password Standards"

With the modernization of the CJISSECPOL, new Identification and Authentication (IA) requirements were incorporated into version 5.9.2 released in December 2022. Memorized Secret (password) authenticator requirements were added which included the previous advanced password standards. The previous basic password standards below were also carried forward into the new requirements.

- Not be a proper name
- Not be the same as the Userid
- Expire within a maximum of 90 calendar days
- Not be identical to the previous ten (10) passwords
- Not be displayed when entered

Basic Password Standards do not meet the new authenticator requirements. Agencies that are operating under those standards may continue to do so until **September 30, 2024**.

Security Control Priority and Implementation Deadlines

As the security controls in the CJISSECPOL are modernized, agencies have been unclear on which controls should be implemented in a particular order. Previously, modernized security controls were assigned deadlines for auditability based on the release date of the version they first appear in the CJISSECPOL and how that date falls relative to the FBI CJIS Audit Unit's (CAU) audit schedule which begins on October 1 of each fiscal year.

The Adversarial Tactics, Techniques, and Common Knowledge, or MITRE ATT&CK, is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. Using MITRE ATT&CK data and cross-mapping it to the National Institute of Science and Technology (NIST) Special Publication (SP) 800-53 Rev. 5.1, Security and Privacy Controls for Information Systems and Organizations, moderate security controls, the following priorities for implementation were developed:

- **Existing** – Existing CJISSECPOL requirement that are currently auditable.
- **Priority 1 (P1)** – Priority 1 controls are determined to be the most critical and will be auditable starting on October 1, 2024. Analysis shows that these controls considerably improve your security posture against known active attacks.
- **Priority 2 (P2) – Priority 4 (P4)** – Priority 2, Priority 3, and Priority 4 will fall into a zero-cycle audit status. The zero-cycle begins October 1, 2024, and ends September 30, 2027.

Each modernized control is marked with one of the above. Non-modernized sections do not have markings but are considered “existing” requirements and continue to be auditable.

The zero-cycle audit controls encompass all new modernized controls not previously in the CJISSECPOL and not identified as being Priority 1 [P1]. The zero-cycle controls account for roughly 56 percent of all controls which will significantly reduce the initial burden on agencies while allowing time to enhance security posture. These controls will be auditable after the zero-cycle audit period above has lapsed.

Agencies can further use the recommended priority code designation associated with each security control to assist in making decisions for control implementation. A Priority Code 2 [P2] control has a higher priority for implementation than a Priority Code 3 [P3] control; a Priority Code 3 [P3] control has a higher priority for implementation than a Priority Code 4 [P4] control. This recommended prioritization sequencing helps ensure that security controls upon which other controls depend are implemented first, thus enabling organizations to deploy controls in a more structured and timely manner in accordance with available resources.

The IJIS Institute has the complete Webinar available for viewing which address CJIS Update information. [Click here to access the video.](#)

Please contact the NC SBI, CJIS Information Security Office at servicedesk@ncsbi.gov with any questions.