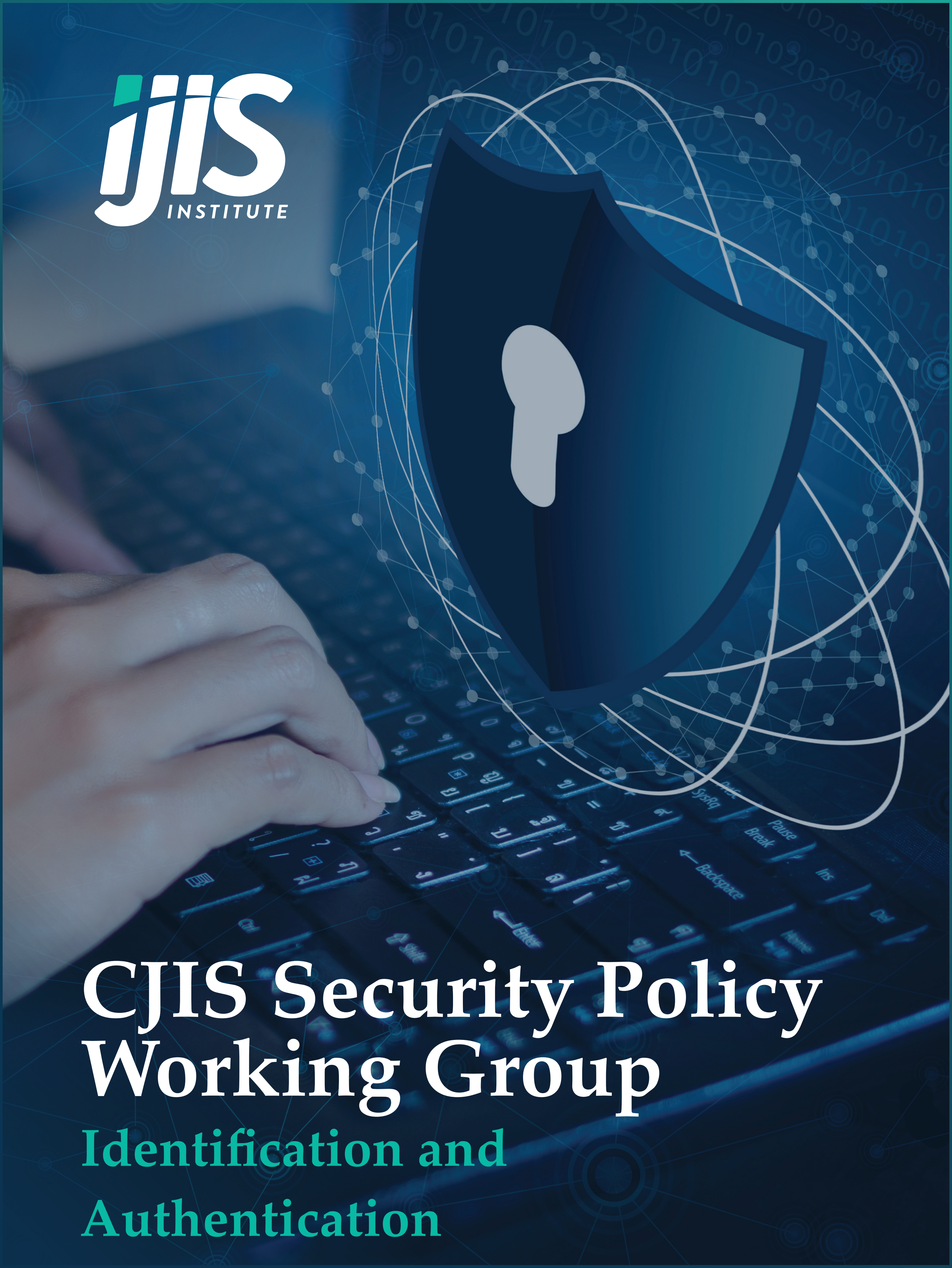


CJIS Security Policy Working Group

Identification and Authentication

Acknowledgements

This document is result of a partnership between the IJIS Institute and the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Division. The IJIS Institute is a nonprofit collaboration network that brings together innovative thinkers from the public and private sectors, national practice associations, and academic / research organizations working together to solve public sector mission, information sharing, policy and technology challenges.

IJIS Mission

To drive public sector technology innovation and empower information sharing to promote safer and healthier communities.

IJIS CJIS Security Policy Work Group Roster

Charlie Schaeffer, Chair	*Microsoft/Azure*
Jens Black	*Motorola Solutions*
Gerard Britton	*Enforsys Inc.*
Jeff Campbell	*FBI CJIS*
Ed Claughton	*PRI Management Group*
Monty Coats	*South Carolina Law Enforcement Division (SLED)*
Holden Cross	*FBI CJIS*
Brian DaSilva	*Mark43*
Matthew Doherty	*Sikich*
Jim Emerson	*NW3C*
Jason Emineth	*equivant*
Gerard Gallant	*Amazon Web Services*
Mike Lesko	*NEC*
Catherine Miller	*Montgomery County Maryland Police*
Maury Mitchell	*Alabama Law Enforcement Agency*
JC North	*Nlets*
Greg Park	*Livermore Police Department, CA*
Bill Philips	*Nlets*
Rob Serio	*Computer Projects of Illinois*
John Tomme	*Innova Solutions*
George Vit	*South Brunswick, NJ Police Department*
Catherine Watson	*AT&T*
Chris Weatherly	*FBI CJIS*

Comments and Questions? They are always welcome! Please contact the IJIS Institute at **info@ijis.org** or **703-726-3697**.

Introduction

The CJIS Security Policy serves as a critical resource for criminal justice agencies by offering guidelines and best practices to protect the integrity, confidentiality, and availability of Criminal Justice Information (CJI). It provides rigorous security requirements, policies, and controls that must be implemented to maintain the trust and reliability of those maintaining and accessing this information. The CJIS Security Policy incorporates executive orders, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) recommendations, and nationally recognized guidance from the National Institute of Standards and Technology.

As technology and innovation continue to advance at an unprecedented pace, ensuring the security of sensitive information is paramount for entities storing and requesting access to CJI. With these critical needs in mind, the Federal Bureau of Investigation (FBI) continues to update the Criminal Justice Information Services (CJIS) Security Policy to provide a comprehensive framework for safeguarding data in an ever-changing environment.

Given the complex and constantly evolving policy requirements, it is imperative to have avenues to simplify and educate the stakeholder community, which includes but is not limited to criminal justice and law enforcement agencies, private sector service providers, nonprofit and academia organizations supporting the public sector community. The IJIS Institute, in partnership with the FBI CJIS Division, continues to collaborate in order to meet public sector mission goals.

Purpose of this Document

In support of and collaboration with the FBI's CJIS Division, the IJIS Institute constituted this Working Group to help address the complexity of the most recent updates to the CJIS Security Policy. Through collaboration of subject matter experts from public sector agencies, industry service providers, and supporting nonprofit organizations, these publications aim to provide template guidelines assisting agencies update their policies, procedures, and ultimately overall security measures. This publication specifically focuses on changes to the Awareness and Training sections of CJIS Security Policy version 5.9.2.

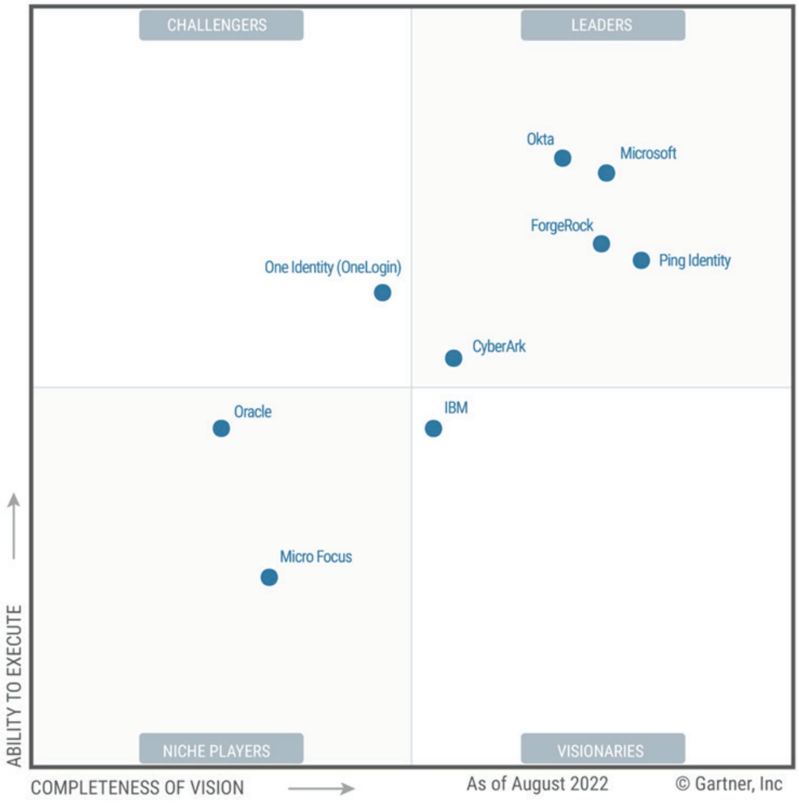
IA Identification and Authentication

Summary of changes

- Modernize the CJIS Security Policy requirements for:

  Identification and Authentication Use of Originating Agency Identifiers in Transactions and Information Exchanges, Policy and Procedures, Identification and Authentication (Organizational Users), Device Identification and Authentication, Identifier Management, Authenticator Management, Authentication Feedback, Cryptographic Module Authentication, Identification and Authentication (Non-Organizational Users), Re-Authentication, and Identity Proofing.

  <u>Note:</u> In many cases, public safety agencies outsource the functions of Identification and Authentication to a Credential Service Provider (CSP). A CSP is a trusted entity that verifies and authenticates the identity of individuals or entities. A Computer-Aided Dispatch (CAD) system, Record Management System (RMS), or a message switch can be considered a CSP as they provide authentication and authorization services to users of that specific system. Active Directory is a directory that manages user accounts and access control policies like CSPs. While it manages authentication and authorization, Active Directory is limited to Windows-based environments and does not manage digital certificates or signatures. Agencies should consider CSPs that offer solutions not limited to their specific system (CAT, RMS, Message Switch) or a specific environment (Active Directory). The following graph shows the most known vendors by Gartner 2022 Access Management.



Source: Gartner (November 2022)

IA-0 Use of Originating Agency Identifiers in Transactions and Information Exchanges

Summary of changes:

- IA-0 makes no changes to requirements except that this section will be moved to IA-3.

IA-1 Policy and Procedures Identification and Authentication

New policy format and requirements based on NIST SP 800-53b.

NIST Policy Primer

As the CJIS Security Policy aligns with the NIST SP 800-53b Moderate baseline, the requirements for and format of agency security policy changes, and the emphasis on documenting procedures is heightened.

SP 800-53 groups related security controls into families such as System and Information Integrity (SI), Security Awareness and Training (AT), Media Protection (MP), Identification and Authentication (IA), and so on.

Each control in a family is numbered, and the first control in each family calls for a policy that specifies the implemented controls along with coverage of the purpose and scope of the policy, agency leadership's commitment to the policy, and the specific duties called for by the policy and the roles, groups, or personnel that are responsible for them.

The intent of this document is to give a quick introduction to writing NIST 800-53 compatible security policies and procedures. Core policy sections are in **bold**, and the example text for the sections is in *italics*.

1. **Purpose**
    a. Things to consider:
        i. The "why" of the policy
        ii. Summarize the primary objective(s)
        iii. How does the policy fit with other agency policies, and/or into larger security/compliance efforts

b. Guidance/Examples

i. *In accordance with AGENCY standards, an Identification and Authentication policy is set in place to comply with the requirements set for by the CJIS Security Policy.*

ii. *To protect AGENCY data, each user, machine, software component, or any other entity shall be uniquely identified and authorized following the rules of least privileged access. The purpose of this policy is to establish guidelines and procedures to ensure the confidentiality, integrity, and availability of the AGENCY's information and systems.*

2. Scope

a. Things to consider:

i. To whom does the policy apply?

ii. Does the policy cover people, systems, devices, networks, or a combination?

iii. If the policy applies to personnel, are any personnel specifically exempted?

iv. Are there any external personnel (contractors, consultants, service providers, partners, etc) with unescorted access to systems or facilities? In CSP, these personnel are generally covered by the policy if they have access to systems, networks, devices, or facilities.

b. Guidance/Examples

i. *This policy applies to all (AGENCY) personnel, contractors, and any third parties with access to (AGENCY) facilities, systems, and/or networks.*

3. Roles and Responsibilities

a. Things to consider:

i. In the agency, who is ultimately responsible for the specific security functions required by the policy?

ii. Who manages/maintains tools relevant to the effort?

iii. Who documents the effort?

iv. Who maintains records or performs periodic reviews of the policy and any documentation, procedures, or audit records/logs?

v. Generally, it is better to note a team or position that holds responsibility rather than specific individuals (by name).

b. Guidance/Examples

i. *RACI (Responsible, Accountable, Consulted, Informed) charts can be quite useful for documenting roles and responsibilities. (Information on RACI charts can be found at RACI Charts - How-to Guide and Templates)*

ii. *Example AT RACI of section 5.6:*

	CJIS ISO	**Human Resources**	**Training**	**Information Security Services**	**AGENCY Personnel**	**Frequency**
Develop and implement Security and privacy policies at the organization level	A	C	I	R	C	
Review and update Identification and authentication controls at the organization level	A	C	I	R	C	
Create and implement a policy following any security incidents involving unauthorized access to CJI or systems used to process, store or transmit CJI data	A	C	I	R	C	
Investigate and report any security incidents involving unauthorized access to CJI or systems used to process, store or transmit CJI data (procedures)	A	I			R	Immediately
Create and implement a Risk management strategy	A	C	I	R	C	
If needed, create and implement procedures for security and privacy programs	A	C	I	I	R	
Update policies and controls to account for new assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines	A	C	I	R	C	Immediately

4. **Management Commitment**
    a. Things to consider:
        i. This statement can be stated as part of an overview, summary, or introduction to the policy
        ii. Why is it important that the policy exist and be observed?
        iii. Why is this function important to the agency?

    b. Guidance/Examples
        i. *Information is a valuable (AGENCY) asset and must be protected from unauthorized disclosure, modification, or destruction. Initial and ongoing security awareness and training for (AGENCY) personnel is a vital component of an overall approach to the secure handling, storage, and processing of sensitive data and compliance with the CJIS Security Policy.*

5. **Controls and Requirements**
    a. This section can also be labeled as **Policy**.
    b. Things to consider:
        i. While it is generally acceptable for agencies to simply "copy and paste" the relevant section from CSP, the outcome of one or more agency leaders reviewing the CSP material through the lens of the agency's overall purpose and objectives tends to be a policy that is clearer to agency personnel and more easily integrated into agency operations.
        ii. It is generally advisable to specify a technology that must be implemented over specifically dictating a given tool or solution (i.e., 'malicious code protection' as opposed to 'ACME Anti-Virus'). Generally, a policy should advise/require the use of a given technology, while procedures deal with specific products that might be in use.
        iii. The policy itself represents the first control in the family, and as such does not need to be reflected IN the policy.

    c. Guidance/Examples
        i. *Ensure that each control in the CSP section is referenced and restated as to how it is implemented at the agency.*
        ii. *If the agency currently goes beyond the CSP requirements, or plans to, this should also be reflected in policy.*

iii. Reference any relevant timelines or required repetitions (training is required prior to granting access to CJI and must be repeated annually; training records must be maintained for three years to accommodate the triennial audit cycle).

iv. For Role-Based Training (AT-3), it is acceptable and may be helpful to group specific agency roles with their respective training levels, updating as roles are added or changed.

v. As the policy must be reviewed, at a minimum, on an annual basis, it is good to include a simple table at the end of the document that tracks the dates of review and changes, along with who made and/or approved the change.

Procedure Primer

Along with the new policy requirements, the new CJISSECPOL version also places more emphasis on the need for procedures documenting how to perform tasks associated with implementation and management of implemented security controls.

1. Things to consider:
    a. Procedures should provide enough detail for a person with basic knowledge of the system or technology to carry out the task.
    b. Tasks performed by all personnel (such as accessing a security training application like CJISOnline) tend to benefit from screenshots, but policies targeted to roles such as system or network administrators or technical security staff generally won't require them.
    c. Document tools and access required, key points of contact if difficulty is encountered (this is especially helpful for procedures that would be used by all personnel), and the basic steps required to perform the task

2. Guidance/Examples
    a. The following is basic structure that can be used for procedures. It can be adopted as-is, but it is recommended to tailor it to suit the specific needs of the agency.
        i. Objective
            1. Summarize the task that the procedure documents
        ii. Tools and Access
            1. List any required tools, applications, websites, etc., and specify the required access level. It can be helpful to include contact information for the person/team that controls this access.
        iii. Procedure
            1. Give an overview of the steps required to complete the task.
            2. Procedures for tasks carried out by junior personnel and non-technical staff will generally need more detail than those intended for senior or technical staff.
        iv. Revision History
            1. As with the policy, keep a simple table at the end of the document.
            2. As with the policy, procedures may be reviewed in your audit.

IA-2 Identification and Authentication (Organizational Users)

Summary of changes

- New control
- Users should have a unique identifier and authorization.
- Users can be internal, contractors and guess researchers.
- Group accounts are allowed, but users should be able to be identified inside groups.
- VPNs are considered part of the internal network.

Control Enhancements:

- **(1) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS**
    - MFA: Something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric).
    - Privileged account: Accounts with elevated levels of access and permissions to critical systems, applications, or data within the agency.
    - Step-Up authentication: A security mechanism that requires a user to provide additional authentication factors beyond the initial login credentials to access privileged data.
- **(2) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS.**
    - Non-Privileged account: User accounts with limited access to an Agency system, application, and data.
- **(8) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCESS TO ACCOUNTS — REPLAY RESISTANT**
    - Replay resistant: A security mechanism that prevents the interception or the reuse of data to gain access to systems or applications.
- **(12) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS**
    - PIV: Personal Identity Verification

IA-3 Identification and Authentication

Summary of changes

- New control
- Devices should have a unique identifier.
- Devices can be internal or external.
- The agency is in control of the strength of the authentication mechanism based on business requirements as long as they are documented in the policy.

IA-4 Identifier Management

Summary of changes

- New control
- Identifiers include individual, group, role, service, or device
- Management includes receiving authorization, selecting, assigning, and preventing reuse (for one year) of the identifier.
- Individual identifiers do not apply to shared system accounts.

Control Enhancements:

- **(4) IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS**
  - Users need to be identified as Agency or Nonagency
  - Characteristics that identify the status of individuals include contractors, foreign nationals, and non-organizational users.

IA-5 Authenticator Management

Summary of changes

- New control
- This section includes the management of system authenticators and rules regarding the use of Authenticator Assurance Level 2 (AAL2), the use of biometrics as part of Multifactor authentication, and Authentication binding.
- Reauthentication is required every 12 hours during an extended usage session.
- Reauthentication is following any period of inactivity lasting 30 minutes or longer.
- Create and follow record retention policies.

- Create and follow Privacy requirements.
- Create risk management processes.
- Requirements regarding session management, including session binding and re-authentication.

Control Enhancements:

- **(1) AUTHENTICATOR MANAGEMENT | AUTHENTICATOR TYPES**
- **(a) Memorized Secret Authenticators and Verifiers**
    - Create a non-allowed password dictionary.
    - New password after account recovery.
    - Long passphrases preferred that include spaces and printable characters.
    - Rules around password creation, expiration, reuse, and making it secret.
    - If using memorized secrets, they must be eight (8) characters at a minimum.
    - If using a Random number generator at a minimum of six (6) characters
    - Knowledge-based authentication is not allowed.
    - Maximum five (5) failed attempts.
- **(b) Look-Up Secret Authenticators and Verifiers**
    - A look-up secret authenticator is defined as a time-based, high-quality random bit generator that provides an additional factor for authentication.
- **(c) Out-of-Band Authenticators and Verifiers**
    - An out-of-band authenticator uses a separate channel to send a verification code to provide an additional factor for authentication.
- **(d) OTP Authenticators and Verifiers**
    - One-time password (OTP) is a one-time code generated to be used as an additional factor for authentication.
- **(e) Cryptographic Authenticators and Verifiers (including single- and multi-factor cryptographic authenticators, both hardware- and software-based)**
    - This section describes rules for software and hardware-based authenticators.
- **(2) AUTHENTICATOR MANAGEMENT | PUBLIC KEY BASED AUTHENTICATION**
    - Public key Infrastructure (PKI) is a cryptographic authenticator used primarily for machine-to-machine authentication, individuals (PIV cards), and devices.
- **(6) AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS**
    - Type of authentication is proportionate to the data that can be accessed and the security mechanism put in place to get access to the data.

IA-6 Authentication Feedback

Summary of changes

- New control
- Obscure feedback of authentication refers to hiding the input of information during the authentication process; for example, a password shows the letter for a few milliseconds, and then it quickly changes to asterisks.

IA-7 Cryptographic Module Authentication

Summary of changes

- New control
- A cryptographic module is a self-contained unit that contains cryptographic algorithms, and it is used to provide security services to verify the integrity and authenticity of the transaction.

IA-8 Identification And Authentication (Non-Organizational Users)

Summary of changes

- New control
- Non-Organizational users are those considered outside of the organization's boundaries. These users should be carefully vetted before allowing access to federal systems, including security, privacy, scalability, and practicality of the need for access.

Control Enhancements:

- **(1) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES**
    - PIV: Personal Identity Verification, a credential issued by a federal agency for logical and physical access control systems.
- **(2) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF EXTERNAL AUTHENTICATORS**
    - External authenticators are allowed if they meet CJISSECPOL requirements. These authenticators shall be NIST-Complaint
    - Agency shall maintain a list of accepted external authenticators.
- **(4) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF DEFINED PROFILES**
    - Standards allowed for interconnection of external authenticators are SAML and OpenID Connect.

IA-11 Re-Authentication

Summary of changes

- New control
- Reauthentication shall occur when a device locks, changes to roles, authenticators, credentials, security categories of systems change, the execution of privileged functions occurs, or every 12 hours.

IA-12 Identity Proofing

Summary of changes

- New control
- Identity proofing is a way to identify an individual as a unique ID. Users should be given an appropriate Identity assurance level based on the user requirements.
- Identity proofing evidence shall be collected, validated, and verified.

Control Enhancements:

- **(2) IDENTITY PROOFING | IDENTITY EVIDENCE**
  - Provide documentary evidence or a combination of documents and biometrics to prove identity.
- **(3) IDENTITY PROOFING | IDENTITY EVIDENCE VALIDATION AND VERIFICATION**
  - This section includes rules and controls that should be included to validate and verify an identity. For example, rules to safeguard the identity, Management of Personal Identifiable Information (PII), privacy, retention, minors, biometrics, training, and support.
- **(5) IDENTITY PROOFING | ADDRESS CONFIRMATION**
  - Use of out of band methods are recommended.
  - Validation of source address (or authoritative source) is required.
  - IAL2 has specific requirements to be followed.