Criminal Justice Information Services (CJIS)

State of Texas – CJIS Requirements Companion Document

CJIS Security Policy version 5.9.4

Revised: May 29, 2024

The essential premise of the CJIS Security Policy (CJISSECPOL) is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJISSECPOL provides guidance for the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI. The CJISSECPOL 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 and noncriminal justice services and information.

The CJISSECPOL is going through a policy modernization effort to align with National Institute of Standards and Technology (NIST) 800-53 revision 5, which are the standards for Security and Privacy Controls for Information Systems and Organizations. NIST is responsible for developing information security standards and guidelines, including risk-based requirements for federal information systems.

The CJISSECPOL may be used as the sole security policy for the agency. The State of Texas has enhanced the CJISSECPOL, posted on our website as the State of Texas CJIS Security Policy Supplement, and the local agency may complement the CJISSECPOL, and the Texas supplement, with a local policy, or the agency may develop their own stand-alone security policy; however, the CJISSECPOL shall always be the minimum standard. State, Local, Tribal, Territorial, and Federal agencies may augment or implement more stringent policies or requirements. The agency shall develop, disseminate, and maintain formal, documented policy and procedures to facilitate the implementation of the CJISSECPOL and, where applicable, the State and local security policies. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. Procedures developed for CJISSECPOL areas can be developed for the security program in general, and for a particular information system, when required. Each agency faces unique risk to that agency. It is quite possible that several agencies could encounter the same type of risk however depending on resources would mitigate that risk differently. In that light, a risk-based approach can be used when implementing these requirements.

The fully modernized CJIS Security Policy is expected to consist of eighteen Security Control Families:

The page numbers in italics reflect where these control families are located within CJISSECPOL v5.9.4.

AC (Access Control) *(page 37)*
AU (Audit & Accountability) *(page 27)*
CM (Configuration Management) *(pending release)*
IA (Identification & Authentication) *(page 58)*
MA (Maintenance) *(page 193)*
PE (Physical & Environmental Protection) *(page 142)*
PS (Personnel Security) *(pending release)*
SA (System & Services Acquisitions) *(page 180)*
SI (System & Information Integrity) *(page 181)*
AT (Awareness & Training) *(page. 11)*
CA (Security Assessment & Authorization) *(pending release)*
CP (Contingency Planning) *(page 206)*
IR (Incident Response) *(page 19)*
MP (Media Protection) *(page 136)*
PL (Planning) *(page 198)*
RA (Risk Assessment) *(page 218)*
SC (System & Communications Protections) *(page 152)*
SR (Supply Chain Risk Management) *(pending release)*

It's highly suggested the agency maintains a binder/book to keep track of the documentation requirements for each of the eighteen security control families. The agency may also want to include any SaaS Assessments and/or On-Premise Assessments that have been completed for your agency. This way, when the technical auditors show up at your agency for an audit, literally throw the book at us… it does make the audit go much smoother and shows how prepared the agency is.

The intent of this Texas version of the requirements document is an effort to present the security controls of the current version of the CJISSECPOL in a slightly less technical format with a target audience being the head of small to mid-size law enforcement agencies, as well as the agency Organizational Personnel with Security Responsibilities, currently the

agency appointed Local Agency Security Officer (LASO). Hopefully, the agency LASO is not also assigned as the TLETS Terminal Agency Coordinator (TAC). If so, as you review this document you will hopefully realize, an agency LASO needs to be a very technical position, appointed by the head of the agency, and can be assigned to University, ISD, City, or County IT support, even a vendor can be an agency appointed LASO, yet if a vendor is appointed, you might need to increase the agency budget because a vendor that wears a LASO hat is going to be very busy. As mentioned, the head of the agency can appoint as many LASO's as needed. As you review this document, and the related Discussion sections in the CJISSECPOL, the agency may also want to consider appointing personnel outside of the law enforcement agency, such as areas in which the outside personnel may have security responsibilities with the law enforcement agency, which may be why the APB is discussing changing the LASO to simply be "Organizational Personnel with Security Responsibilities". Also, agency TACs are normally Dispatch Supervisors that can, and do, work miracles, every day, yet as you all know, they have both hands full, way too many hats, and very few TACs somehow manage to have the required technical skills to also be an agency LASO. So, if that's you, and you wear both the TAC and LASO hat, if you have any questions regarding the CJISSECPOL, please use that phone that you are already always on and consider that you have a priority line with the CJIS Security Office and give us a call (512) 424-5686.

This document also includes insight into the controls in which the State of Texas CJIS ISO is focusing our agency technical compliance efforts, which is obviously towards the controls where the agencies appear to have the most difficulties maintaining compliance. Since there is an ever-increasing requirement on technical skills at the agency, which in many ways can be attributed towards the enhancements of the CJISSEPOL, yet the need for more technical support also needs to be attributed to the agency choices in technology. This document also includes Texas CJIS ISO suggestions on the level of IT Support that may/will be needed to implement the specific security controls, where the basis for making such determinations was focused on the smaller agencies with little to none, IT Support.

As the CJIS ISO for the State of Texas, I suspect many agencies will likely be scratching their heads, or throwing their arms up, as to how the agency can implement many of the new security controls. Please remember, the agency can always consider a risk-based approach towards implementation of these security controls. If the agency is unclear if the methods in which the agency plans to implement the security controls meet the CJIS requirements, usually the vendor is the first place the agency should start to assess the controls. Then, work towards documenting how the agency plans to meet the security controls into a security plan and if the assessment is for a new vendor solution, send a request for an assessment to the CJIS Assessment team at cjis.assessments@dps.texas.gov and they will schedule a time to review the assessment questionnaire with the agency. Please remember, DPS cannot be part of an agency solicitation, request for proposal, or be involved in the agency vendor selection process. So, once the agency has selected a vendor solution that will be used to either process, store, and/or transmit CJI, has fully executed the CJIS Security Addendum with the vendor, conducted Personnel Screening on all the vendor personnel with unescorted access to agency secure location or unencrypted CJI, and validated the vendor personnel has successfully completed the appropriate awareness training, DPS will assist the agency in completing the CJIS Assessment process so the agency obtain an interface to TLETS, if needed, and go live with the new vendor solution.

DPS personnel cannot recommend vendor solutions to an agency. In addition, we will not discuss an agency solution or proposed solution with a vendor unless an agency representative is on the call, or at least courtesy-copied on an email. If possible, the agency personnel that should be involved in any discussions with a vendor and DPS should also be identified on the agency Terminal Connection Report (TCR). The agency TAC will know how to update the TCR. DPS will follow DPS procedures to ensure we do not make agency changes unless it is approved by a person listed on the agency TCR or confirmed by the head of the agency. If the agency is not connected to TLETS, we request the head of the agency document and submit the agency choice(s) for LASO to the CJIS Assessments team email account listed above, and the contacts will be placed in the agency file.

As the agency attempts to maintain CJIS compliance with the enhanced policy, do the best your agency can do, and if you think the agency is falling short of compliance, please reach out to the CJIS Security Office (512) 424-5686 as soon as possible, we will work with the agency towards obtaining compliance, which is beneficial for all of us.

As a possible result of the technical requirements within the modernized CJISSECPOL, many small agencies may feel forced to move to a cloud-based infrastructure where the cloud service providers (CSP) perform many of the technical

services now required under the CJISSECPOL. A cloud-based solution can be an excellent choice for many agencies, but it is not a one size fits all. In addition, many agencies may choose to consolidate and/or connect to TLETS through a larger agency that has IT Support that can perform the services required under the CJISSECPOL. That too can be an excellent option for an agency, but remember, when you are connecting to TLETS through another agency, the hosted agency is subject to the hosting agency's policies. As with the flexibility the agency has in methods in which they can meet the requirements of the CJISSECPOL, the agency has a lot of flexibility working with vendors, cloud-service providers, and other agencies.

This document is not intended to replace or be an authoritative source of the CJISSECPOL requirements. Always refer to the CJISSECPOL as the official FBI CJIS Security Policy requirements.

I would appreciate it if you would let me know if you find any discrepancies or errors within this document.

I hope you will find this document useful as we work together to provide a more secure environment for us all.

James F. Gore – CJIS ISO – Texas
Senior Director – Compliance and Training Bureau
Crime Records Division
Texas Department of Public Safety
james.gore@dps.texas.gov
(512) 424-7911

WE TRUST BUT VERIFY!

Table of Contents

DOCUMENTS AND RESOURCES

You may download many relevant documents from the DPS CJIS Security Office website:
https://www.dps.texas.gov/section/crime-records/cjis-documents

CJIS Security Policy v5.9.4

Please remember, the CJISSECPOL is in the modernization process to align with the NIST 800-53r5 security controls. There are discrepancies between the Appendixes and the Requirements Companion document. Please consider the CJISSECPOL to be the authoritative source if you have concerns with any discrepancies found within the CJISSECPOL Appendixes and/or Requirements Companion document. This includes, sanctionable dates.

CJIS Security Policy Requirements Companion Document

As Chris Weatherly says, "This is the stuff without the fluff". If you are not familiar with the CJISSECPOL, I have always recommended that the agency should start with the Requirements Companion Document. Especially if the agency is implementing a SaaS solution in a cloud-based environment. Review the security controls in which you are trying to assess, and if you need more information, refer to the Discussion portion of the security control in the CJISSECPOL. If you need further clarification, you may refer to NIST 800-53r5 to try and understand the original intent of the security control. If you still have questions please contact the CJIS Security Office security.committee@dps.texas.gov, the CJIS Assessment Team at cjis.assessments@dps.texas.gov or give us a call at (512) 424-5686.

NOTE: We do not provide approvals for agency changes to systems used to process, store, or transmit CJI over the phone. All requests for agency changes should be sent to cjis.assessments@dps.texas.gov

State of Texas – CJISSECPOL- Requirements Companion Document

This document, the one you are currently looking at, is an effort to present the security controls of the current version of the CJISSECPOL in a slightly less technical format with a target audience being the head of small to mid-size law enforcement agencies, as well as the agency Organizational Personnel with Security Responsibilities, currently the agency appointed Local Agency Security Officer (LASO).

The Texas version of the CJIS Security Addendum

The CJIS Security Addendum is a legal addendum to the contract the agency has with a vendor, and vendor subcontractors. As with any legal document, it is not valid if it is not fully executed. We require the agency to submit a fully executed Security Addendum at time of audit, for all vendors providing services to the agency where the vendor may have unescorted access to agency secure locations, access to unencrypted CJI, or access to systems used to process, store, or transmit CJI. The Texas version of the CJIS Security Addendum includes PII on the FBI Certification Page that is to be used by the agency to ensure positive identification of the individual for conducting national fingerprint-based background checks. In addition, the Texas version of the Security Addendum includes:

Page 1 – The Agency and Vendor/Contactor Identification Information.

Pages 2-6 – Legal jargon that can only be revised by the FBI.

Page 7 – The FBI Certification Page. This must be fully executed by all vendor personnel providing services to the agency. This page legally binds the individual to the requirements of the CJIS Security Addendum.

> NOTE: The FBI Certification Page of the Security Addendum clearly states the vendor personnel are familiar with the Security Addendum, NCIC Operating Manual, CJIS Security Policy, CFR 28:20, and they personally agree to be bound by their provisions. These documents can also be downloaded from the DPS Security Office website.

Page 8 – Texas Signatory Page. This is where the agency, Vendor/Contractor/Sub-Contractors sign the document acknowledging that it is part of the contract between the agency and the vendor/contractor/sub-contractors.

The Texas CJIS Security Policy Supplement

As the CJISSECPOL states in section 1.3, "The CJISSECPOL shall always be the minimum standard. State, Local, Tribal, Territorial, and Federal agencies may augment or implement more stringent policies or requirements."

As such, the State of Texas has enhanced the CJISSECPOL, as noted in the Texas CJIS Security Policy Supplement.

APB Topic Request Form

This document may be used to request a topic for discussion by the CJIS Advisory Policy Board.

TCIC System Access Chart

These are State requirements to be used by the agency to determine eligibility of personnel requesting access to Texas CJIS Systems. Once again, the agency may enhance these requirements, but they may not lessen these requirements.

The local agency administrator (i.e., Chief, Sheriff, or their equivalent) may request a wavier that would allow access to the DPS/FBI systems. To qualify for a waiver, an individual must have been convicted or placed on community supervision for a Class B misdemeanor at least five (5) years prior to the application. The agency head must articulate in writing the mitigating circumstances that exist with the case and must attest to the value of the individual to the criminal justice community. The request shall also include a statement that the public interest would be served by reducing the denial period. These requests shall be addressed to the CJIS Systems Officer (CSO) and emailed to the following resource address: security.committee@dps.texas.gov

Security Incident Response Form

The agency is required to notify DPS with one (1) hour after discovery by contacting the Operations Information Center (OIC) at (888) 377-6420. After notification to the OIC, the Security Committee will contact the agency, determine if the agency requests any assistance from DPS Cyber Security, and request the Incident Response Form be submitted to DPS when there is confidence the agency email system is not compromised, or infected.

Sample Management Control Agreement for Technical Services

The Management Control Agreement is used by the agency to ensure the agency maintains management control of all systems used to process CJI. This document is where the agency documents what services the other governmental entity is authorized by the agency to perform.

For example: If a County Sheriff's Office utilizes County IT, the Management Control Agreement is required between the County Sheriff's Office and the County IT Department. If a City Police Department utilizes City IT, the Management Control Agreement is required between the Police Department and the City IT Department. If a University Police Department utilizes the University IT, the Management Control Agreement is required between the University Police Department and the University IT Department. Also, if one of the above utilize a vendor who is contracted by County, City, or University, the Management Control Agreement is still required, in addition to a CJIS Security Addendum between the vendor and the agency. This may prevent a government entity from telling IT to put a VNC client on the Chiefs computer to monitor his/her activities…

Sample Management Control Agreement for Dispatch Services

The Management Control Agreement is always required when the agency utilizes another government entity to perform law enforcement services with access to CJI. Including consolidated dispatch centers, where the where a majority of management control remains with a criminal justice agency.

There may be other purposes for a Management Control Agreement, such as forensic services…

The CJIS Technical Listserv.

Agency personnel are encouraged to subscribe to the CJIS Technical Listserv at the following URL:

https://www.dps.texas.gov/securityreview/AlertRegistration/default.aspx

CJIS Policy Modernization Effort

CJISSECPOL v5.9.1

The FBI officially released CJISSECPOL version 5.9.1 October 1, 2022. This release was limited to the Media Protection security controls. Specifically,

5.8 MEDIA PROTECTION (MP)

MP-1 POLICY AND PROCEDURES
MP-2 MEDIA ACCESS
MP-3 MEDIA MARKING
MP-4 MEDIA STORAGE
MP-5 MEDIA TRANSPORT
MP-6 MEDIA SANITIZATION
MP-7 MEDIA USE

MP-1 POLICY AND PROCEDURES

Current - This control is currently sanctionable for audit.

The -1 Security Control "POLICY AND PROCEDURES" you will find in all eighteen of the new security control families. This is where the agency establishes and documents agency policy, including Purpose, Scope, Roles, Responsibilities, Management Commitment, Coordination among agency entities, Compliance and step by step procedures as to how the policy will be implemented at the agency. It is highly recommended the agency have its own policies and procedures and not rely upon County, City, or University policies to meet these CJISSECPOL requirements, enhanced requirements found in the State of Texas Security Policy Supplement, and any potential Local agency enhanced requirements.

NIST has developed and provided to the FBI sample policies to assist the agencies in developing local agency policies. These sample policies are available for download from the DPS Security Office website (https://www.dps.texas.gov/section/crime-records/cjis-documents) under the Sample Agreements, Policies & Procedures section. Please feel free to use these as a baseline for documenting your agency specific policies. In addition to the agency policies, DPS auditors will be expecting the agency to provide documented procedures as to how the agency is implementing these policies as a deliverable for the agency CJIS audit.

The agency must designate an individual with security responsibilities to manage the development, documentation, and dissemination of the agency policies and procedures, and review and update the policy annually, and after any security incidents.

MP-2 MEDIA ACCESS

Current - This control is currently sanctionable for audit.

This control should already be in effect whereas it simply requires the agency to restrict access to digital and non-digital media to authorized individuals.

MP-3 MEDIA MARKING

Delayed - This control is currently delayed by the FBI.

On July 5, 2023, the FBI advised the state ISO's: "*Due to a recent revelation internal to DOJ/FBI that impact a portion of the media protection standards, the FBI CJIS Audit Unit (CAU)* ***will not start*** *assessing agencies on compliance with MP-3 on October 1, 2023, as noted within CJISSECPOL v5.9.2. In the next release of the CJISSECPOL (v5.9.3), the language will be grayed out until such time the FBI CAU begins assessing agencies on compliance. Prior notice will be provided before MP-3 becomes sanctionable by the CJIS Advisory Policy Board.*"

MP-4 MEDIA STORAGE

Current - This control is currently sanctionable for audit.

Physically control and securely store digital and non-digital media within physically secure locations or controlled areas and encrypt CJI on digital media, using AES 256-bit encryption and centrally control the encryption keys, when physical and personnel restrictions are not feasible; and protect system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

MP-5 MEDIA TRANSPORT

Current - This control is currently sanctionable for audit.

Not much has changed in this control since version 5.9, yet please pay close attention to the documentation requirements. Do you take CJI home or to the court, etc.? If so, document the activities and remember, if you don't have a policy in place to address potential misuse, or loss of media while in transport, you may have limited options for any potential sanctions. Please be sure to document activities associated with the transport of media, such as:

Flash drives
Diskettes
Magnetic tapes
External or removable hard disk drives (Check CID, IA, Intel)
Compact discs
Microfilm
Paper

MP-6 MEDIA SANITIZATION

Current - This control is currently sanctionable for audit.

NOTE: The agency will likely need skilled IT resources to be able to meet this requirement.

Not much has change on this control since version 5.9, basically, sanitize or destroy digital and non-digital media prior to disposal, release out of agency control, or release for reuse using overwrite technology at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals.

MP-7 MEDIA USE

Current - This control is currently sanctionable for audit.

The agency is required to restrict the use of digital and non-digital media on agency owned systems that have been approved for use in the storage, processing, or transmission of criminal justice information by using technical, physical, or administrative controls; and prohibit the use of personally owned digital media devices on all agency owned or controlled systems that store, process, or transmit criminal justice information; and prohibit the use of digital media devices on all agency owned or controlled systems that store, process, or transmit criminal justice information when such devices have no identifiable owner.

CJISSECPOL v5.9.2

The FBI Officially released CJISSECPOL version 5.9.2 December 7, 2022. This release was limited to the Awareness and Training, Identification and Authentication, one critical security control from System and Services Acquisition, and System and Information Integrity. Specifically,

- 5.2 AWARENESS AND TRAINING (AT)
  - AT-1 POLICY AND PROCEDURES
  - AT-2 LITERACY TRAINING AND AWARENESS
    - (2) LITERACY TRAINING AND AWARENESS | INSIDER THREAT
    - (3) LITERACY TRAINING AND AWARENESS | SOCIAL ENGINEERING AND MINING
  - AT-3 ROLE-BASED TRAINING
    - (5) ROLE-BASED TRAINING | PROCESSING PERSONALLY IDENTIFIABLE INFORMATION
  - AT-4 TRAINING RECORDS

- 5.6 IDENTIFICATION AND AUTHENTICATION (IA)
  - IA-0 USE OF ORIGINATING AGENCY IDENTIFIERS IN TRANSACTIONS AND INFORMATION EXCHANGES
  - IA-1 POLICY AND PROCEDURES
  - IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
    - (1) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS
    - (2) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS
    - (8) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCESS TO ACCOUNTS — REPLAY RESISTANT
    - (12) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS
  - IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION
  - IA-4 IDENTIFIER MANAGEMENT
    - (4) IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS
  - IA-5 AUTHENTICATOR MANAGEMENT
    - (1) AUTHENTICATOR MANAGEMENT | AUTHENTICATOR TYPES
      - (a) Memorized Secret Authenticators and Verifiers
      - (b) Look-Up Secret Authenticators and Verifiers
      - (c) Out-of-Band Authenticators and Verifiers
      - (d) OTP Authenticators and Verifiers
      - (e) Cryptographic Authenticators and Verifiers (including single- and multi-factor cryptographic authenticators, both hardware- and software-based)
    - (2) AUTHENTICATOR MANAGEMENT | PUBLIC KEY BASED AUTHENTICATION
    - (6) AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS
  - IA-6 AUTHENTICATION FEEDBACK
  - IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION
  - IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)
    - (1) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES
    - (2) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF EXTERNAL AUTHENTICATORS
    - (4) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF DEFINED PROFILES
  - IA-11 RE-AUTHENTICATION
  - IA-12 IDENTITY PROOFING
    - (2) IDENTITY PROOFING | IDENTITY EVIDENCE
    - (3) IDENTITY PROOFING | IDENTITY EVIDENCE VALIDATION AND VERIFICATION
    - (5) IDENTITY PROOFING | ADDRESS CONFIRMATION

5.2 AWARENESS AND TRAINING (AT)

AT-1 POLICY AND PROCEDURES

Current - This control is currently sanctionable for audit.

This is where the agency establishes and documents agency policy, including Purpose, Scope, Roles, Responsibilities, Management Commitment, Coordination among agency entities, Compliance and step by step procedures as to how the policy will be implemented at the agency.

The agency must designate an individual with security responsibilities to manage the development, documentation, and dissemination of the agency policies and procedures, and review and update the policy annually, and after any security incidents.

AT-2 LITERACY TRAINING AND AWARENESS

Mixed - This control has enhancements that are currently sanctionable and some that are not sanctionable for audit until October 1, 2024.

The agency is required to provide security and privacy literacy training to system users (including managers, senior executives, and contractors) as part of initial training for new users prior to accessing CJI and annually thereafter; and when required by system changes or within 30 days of any security event for individuals involved in the event.

(2) LITERACY TRAINING AND AWARENESS | INSIDER THREAT

Current - This control is currently sanctionable for audit.

Provide literacy training on recognizing and reporting potential indicators of insider threat.

(3) LITERACY TRAINING AND AWARENESS | SOCIAL ENGINEERING AND MINING

Current - This control is currently sanctionable for audit.

Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining. Social engineering is an attempt to trick an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, thread-jacking, social media exploitation, and tailgating.

AT-3 ROLE-BASED TRAINING

Current - This control is currently sanctionable for audit.

NOTE: DPS provides access to cjisonline.com where agency and vendor personnel may take and track awareness training, at no cost to the agency.

The agency is required provide role-based security and privacy training to personnel with the following roles and responsibilities:

- All individuals with unescorted access to a physically secure location.
- General User: A user, but not a process, who is authorized to use an information system.
- Privileged User (ie: TAC): A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform.
- Organizational Personnel with Security Responsibilities (ie: LASO): Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL.

(5) ROLE-BASED TRAINING | PROCESSING PERSONALLY IDENTIFIABLE INFORMATION

Current - This control is currently sanctionable for audit.

The CJISSECPOL is now including Personally Identifiable Information (PII) throughout portions of the policy. PII is not subject to the same security controls as CJI. However, PII is regulated data, like CJI, and as such requires certain protections. This control is to ensure the agency personnel are trained on how to protect PII at the agency.

AT-4 TRAINING RECORDS

Current - This control is currently sanctionable for audit.

The agency is required to document and monitor security and privacy training and retain training records for a minimum of three years. Do not rely upon CJIS Online to meet this requirement whereas CJIS Online does not track agency internal training efforts.

5.6 IDENTIFICATION AND AUTHENTICATION (IA)

IA-0 USE OF ORIGINATING AGENCY IDENTIFIERS IN TRANSACTIONS AND INFORMATION EXCHANGES

Current - This control is currently sanctionable for audit.

The FBI authorized Originating Agency Identifier (ORI) shall be used in each transaction on CJIS systems to identify the sending agency and to ensure the proper level of access for each transaction. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Agencies assigned a limited access ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.

IA-1 POLICY AND PROCEDURES

10/01/2024 - This control is not sanctionable for audit until October 1, 2024.

This is where the agency establishes and documents agency policy, including Purpose, Scope, Roles, Responsibilities, Management Commitment, Coordination among agency entities, Compliance and step by step procedures as to how the policy will be implemented at the agency.

The agency must designate an individual with security responsibilities to manage the development, documentation, and dissemination of the agency policies and procedures, and review and update the policy annually, and after any security incidents.

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Current - This control is currently sanctionable for audit.
NOTE: The agency will likely need skilled IT resources to be able to meet this requirement.
The agency is required to uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

Identification (user id's) must be unique, no sharing of user id's is permitted unless the agency provides documentation as to the rationale specific to AC-14. Account actions must be able to be traced to an individual.
Authentication may be done using passwords (e.g.: memorized secrets-something you know), physical authenticators (e.g.: tokens, cell phones-something you have), biometrics (e.g.: fingerprints-something you are), or multi-factor authentication (MFA) which is two or more of the above listed authenticators.

(1) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS

10/01/2024 - This control is not sanctionable for audit until October 1, 2024
Implement multi-factor authentication (MFA) for access to privileged accounts.

Privileged Accounts are accounts in which the end-user that is authorized, therefore trusted, to perform security relevant functions that the general users are not authorized to perform (e.g.: TAC's with OpenFox Configurator access, IT Support, etc.)

Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows:

- something you know (e.g., a personal identification number [PIN])
- something you have (e.g., a physical authenticator such as a cryptographic private key)
- something you are (e.g., a biometric).

In addition to authenticating users at the system level (i.e., at logon), organizations may employ authentication mechanisms at the application level, at their discretion, to provide increased security. Regardless of the type of access (i.e., local, network, remote), privileged accounts are authenticated using multi-factor options appropriate for the level of risk.

NOTE: Think of this like the System Use Notification message where the end-user is required to see the message prior to gaining access to systems used to process CJI, regardless of method (internal domain, cloud-based). With MFA, the end-user must authentication into the secure network (e.g.: system-level ; typically, the Active Directory domain) using MFA. If the end-user is accessing a system used to process CJI, such as a cloud-based application, without the end-user being required to authenticate at the agency domain, the application must have MFA used to authenticate the end-user.

(2) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
Basically, everyone that logs into the agency secure network, or any system used to process CJI is required to authenticates using multi-factor authentication (MFA). There are no exceptions with the agency secure locations, such as dispatch, and the officers in the units using MDT's are no longer exempt, as they were with advanced authentication, and MFA will be required. Once again, there is no exemption for MFA in the units, or in dispatch.

(8) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCESS TO ACCOUNTS — REPLAY RESISTANT

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

The agency is required to implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts. The agency will need to validate this with the vendor of choice. Replay-resistant techniques include protocols that use nonces (e.g.: arbitrary number used in cryptographic communication that ensures it cannot be reused in replay attacks,) or challenges such as time synchronous or cryptographic authenticators.

(12) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

The agency is required to accept and electronically verify Personal Identity Verification (PIV) cards, DoD Access Cards (CAC), that conform to FIPS 201 and supporting guidance.

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

NOTE: The agency will likely need skilled IT resources to be able to meet this requirement.

The agency is required to uniquely identify and authenticate agency-managed devices before establishing network connections. In the instance of local connection, the device must be approved by the agency and the device must be identified and authenticated prior to connection to an agency asset. This includes devices that are not owned by the agency. Because of the challenges of implementing device authentication on a large scale, organizations can restrict the application of the control to a limited number/type of devices based on mission or business needs.

IA-4 IDENTIFIER MANAGEMENT

Mixed - This control is currently sanctionable, except the reuse of the identifier which is not sanctionable for audit until October 1, 2024.

NOTE: The agency will likely need skilled IT resources to be able to meet this requirement.

The agency is required to manage system identifiers by receiving authorization from organizational personnel with identifier management responsibilities to assign an individual, group, role, service, or device identifier, selecting an identifier that identifies an individual, group, role, service, or device, assigning the identifier to the intended individual, group, role, service, or device, and preventing reuse of identifiers for one (1) year.

Common device identifiers include Media Access Control (MAC) addresses, Internet Protocol (IP) addresses, or device-unique token identifiers. The management of individual identifiers is not applicable to shared system accounts, such as “Administrator”. Typically, individual identifiers are the usernames of the system accounts assigned to those individuals.

(4) IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

The agency is required to manage individual identifiers by uniquely identifying each individual as agency or nonagency.

Characteristics that identify the status of individuals include contractors, foreign nationals, and non-organizational users. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor.

IA-5 AUTHENTICATOR MANAGEMENT

NOTE: The agency will need skilled IT resources to be able to meet this requirement.

These security controls are where the agency will need to work with the agency vendor of choice to ensure compliance. The agency needs to have the vendor explain, in writing, how the agency meets each of these security controls, because the agency will have to be able to explain to the DPS auditor and/or assessor, how the vendor solution meets these security controls. As is explained throughout this section of the CJISSECPOL, there are numerous options for the agency to be able to maintain compliance. Please work with your vendor(s) to determine which solutions may work best for your agency.

For your convenience, I have provided the list of controls grouped by the sanctionable dates. However, due to the complexity and quantity of the following controls, it is very difficult to restate the controls in laymen's terms or provide much more of an explanation. Please refer to the CJISSECPOL to review the discussion section of each specific security control for further information.

The agency is required to manage system authenticators by:

CURRENT - These controls are currently sanctionable for audit.

b. Establishing initial authenticator content for any authenticators issued by the organization;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;

e. Changing default authenticators prior to first use;

f. Changing or refreshing authenticators annually or when there is evidence of authenticator compromise;

g. Protecting authenticator content from unauthorized disclosure and modification;

The agency is required to manage system authenticators by:

10/01/2024 - These controls are not sanctionable for audit until October 1, 2024

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and

i. Changing authenticators for group or role accounts when membership to those account changes.

j. Authenticator Assurance Level 2 (AAL2) Specific Requirements

All credential service providers (CSPs) authenticating claimants at Authenticator Assurance Level 2 (AAL2) SHALL be assessed on the following criteria:

(1) Authentication SHALL occur by the use of either a multi-factor authenticator or a combination of two single-factor authenticators.

Nine different authenticator types are recognized, representing something you know (a memorized secret), something you have (a physical authenticator), or combinations of physical authenticators with either memorized secrets or biometric modalities (something you are).

Multi-factor (MF) authentication is required at AAL2.

MF authentication at AAL2 may be performed using the following AAL2 permitted authenticator types: MF OTP Device, MF Crypto Software, or MF Crypto Device; or a memorized secret used in combination with the following permitted single-factor authenticators: Look-Up Secret, Out-of-Band authenticator, SF OTP Device, SF Crypto Software, or SF Crypto Device.

(2) If the multi-factor authentication process uses a combination of two single-factor authenticators, then it SHALL include a Memorized Secret authenticator and a possession-based authenticator.

(3) Cryptographic authenticators used at AAL2 SHALL use approved cryptography. Cryptography is considered approved if it is specified or adopted in a FIPS or NIST recommendation. Since verifiers and cryptographic authenticators must use the same algorithms to successfully authenticate, assessment of the verifier also assesses the authenticators that may be used.

(4) At least one authenticator used at AAL2 SHALL be replay resistant.

Replay resistance is a characteristic of most, although not all, physical authenticators. A given output of the authenticator is required to be accepted for only one authentication transaction.

(5) Communication between the claimant and verifier SHALL be via an authenticated protected channel. This is typically accomplished using the Transport Level Security (TLS 1.2) protocol.

(6) Verifiers operated by government agencies at AAL2 SHALL be validated to meet the requirements of FIPS 140 Level 1.
(7) Authenticators procured by government agencies SHALL be validated to meet the requirements of FIPS 140 Level 1.
(8) If a device such as a smartphone is used in the authentication process, then the unlocking of that device (typically done using a PIN or biometric) SHALL NOT be considered one of the authentication factors.
(9) If a biometric factor is used in authentication at AAL2, then the performance requirements stated in IA-5 m Biometric Requirements SHALL be met.
(10) Reauthentication of the subscriber SHALL be repeated at least once per 12 hours during an extended usage session.
(11) Reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 30 minutes or longer.
(12) The CSP SHALL employ appropriately tailored security controls from the moderate baseline of security controls defined in the CJISSECPOL.
(13) The CSP SHALL comply with records retention policies in accordance with applicable laws and regulations.
(14) If the CSP opts to retain records in the absence of any mandatory requirements, then the CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine how long records should be retained and SHALL inform subscribers of that retention policy.

k. Privacy requirements that apply to all CSPs, verifiers, and RPs.
(1) The CSP SHALL employ appropriately tailored privacy controls from the CJISSECPOL.
(2) If the CSP processes attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively “identity service”), related fraud mitigation, or to comply with law or legal process, then the CSP SHALL implement measures to maintain predictability and manageability commensurate with the associated privacy risk.

l. General requirements applicable to AAL2 authentication process
(1) CSPs SHALL provide subscriber instructions on how to appropriately protect a physical authenticator against theft or loss.
(2) The CSP SHALL provide a mechanism to revoke or suspend the authenticator immediately upon notification from subscriber that loss or theft of the authenticator is suspected.
(3) If required by the authenticator type descriptions in IA-5(1), then the verifier SHALL implement controls to protect against online guessing attacks.
(4) If required by the authenticator type descriptions in IA-5(1) and the description of a given authenticator does not specify otherwise, then the verifier SHALL limit consecutive failed authentication attempts on a single account to no more than 100.
(5) If signed attestations are used, then they SHALL be signed using a digital signature that provides at least the minimum security strength specified in the latest revision of 112 bits as of the date of this publication.
(6) If the verifier and CSP are separate entities (as shown by the dotted line in Figure 6 Digital Identity Model), then communications between the verifier and CSP SHALL occur through a mutually-authenticated secure channel (such as a client-authenticated TLS connection).
(7) If the CSP provides the subscriber with a means to report loss, theft, or damage to an authenticator using a backup or alternate authenticator, then that authenticator SHALL be either a memorized secret or a physical authenticator.
(8) If the CSP chooses to verify an address of record (i.e., email, telephone, postal) and suspend authenticator(s) reported to have been compromised, then...The suspension SHALL be reversible if the subscriber successfully authenticates to the CSP using a valid (i.e., not suspended) authenticator and requests reactivation of an authenticator suspended in this manner.
(9) If and when an authenticator expires, it SHALL NOT be usable for authentication.

(10) The CSP SHALL have a documented process to require subscribers to surrender or report the loss of any physical authenticator containing attribute certificates signed by the CSP as soon as practical after expiration or receipt of a renewed authenticator.

(11) CSPs SHALL revoke the binding of authenticators immediately upon notification when an online identity ceases to exist (e.g., subscriber's death, discovery of a fraudulent subscriber), when requested by the subscriber, or when the CSP determines that the subscriber no longer meets its eligibility requirements.

(12) The CSP SHALL have a documented process to require subscribers to surrender or report the loss of any physical authenticator containing certified attributes signed by the CSP within five (5) days after revocation or termination takes place.

m. Biometric Requirements

(1) Biometrics SHALL be used only as part of multi-factor authentication with a physical authenticator (something you have).

(2) An authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier SHALL be established.

(3) The sensor or endpoint SHALL be authenticated prior to capturing the biometric sample from the claimant.

(4) The biometric system SHALL operate with an FMR [ISO/IEC 2382-37] of 1 in 1000 or better. This FMR SHALL be achieved under conditions of a conformant attack (i.e., zero-effort impostor attempt) as defined in [ISO/IEC 30107-1].

(5) The biometric system SHALL allow no more than 5 consecutive failed authentication attempts or 10 consecutive failed attempts if PAD demonstrating at least 90% resistance to presentation attacks is implemented.

(6) Once the limit on authentication failures has been reached, the biometric authenticator SHALL either:

i. Impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt, or

ii. disable the biometric user authentication and offer another factor (e.g., a different biometric modality or a PIN/Passcode if it is not already a required factor) if such an alternative method is already available.

(7) The verifier SHALL make a determination of sensor and endpoint performance, integrity, and authenticity.

(8) If biometric comparison is performed centrally, then use of the biometric as an authentication factor SHALL be limited to one or more specific devices that are identified using approved cryptography.

(9) If biometric comparison is performed centrally, then a separate key SHALL be used for identifying the device.

(10) If biometric comparison is performed centrally, then biometric revocation, referred to as biometric template protection in ISO/IEC 24745, SHALL be implemented.

(11) If biometric comparison is performed centrally, all transmission of biometrics SHALL be over the authenticated protected channel.

(12) Biometric samples and any biometric data derived from the biometric sample such as a probe produced through signal processing SHALL be zeroized immediately after any training or research data has been derived.

n. Authenticator binding refers to the establishment of an association between a specific authenticator and a subscriber's account, enabling the authenticator to be used possibly in conjunction with other authenticators to authenticate for that account.

(1) Authenticators SHALL be bound to subscriber accounts by either issuance by the CSP as part of enrollment or associating a subscriber-provided authenticator that is acceptable to the CSP.

(2) Throughout the digital identity lifecycle, CSPs SHALL maintain a record of all authenticators that are or have been associated with each identity.

(3) The CSP or verifier SHALL maintain the information required for throttling authentication attempts.

(4) The CSP SHALL also verify the type of user-provided authenticator so verifiers can determine compliance with requirements at each AAL.

(5) The record created by the CSP SHALL contain the date and time the authenticator was bound to the account.
(6) When any new authenticator is bound to a subscriber account, the CSP SHALL ensure that the binding protocol and the protocol for provisioning the associated key(s) are done at AAL2.
(7) Protocols for key provisioning SHALL use authenticated protected channels or be performed in person to protect against MitM attacks.
(8) Binding of multi-factor authenticators SHALL require multi-factor authentication (or equivalent) at identity proofing.
(9) At enrollment, the CSP SHALL bind at least one, and SHOULD bind at least two, physical (something you have) authenticators to the subscriber's online identity, in addition to a memorized secret or one or more biometrics.
(10) At enrollment, authenticators at AAL2 and IAL2 SHALL be bound to the account.
(11) If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then the applicant SHALL identify themselves in each new binding transaction by presenting a temporary secret which was either established during a prior transaction, or sent to the applicant's phone number, email address, or postal address of record.
(12) If enrollment and binding are being done remotely and cannot be completed in a single electronic transaction, then long-term authenticator secrets are delivered to the applicant within a protected session.
(13) If enrollment and binding are being done in person and cannot be completed in a single physical encounter, the applicant SHALL identify themselves in person by either using a secret as described in IA-5 n (12) above, or through use of a biometric that was recorded during a prior encounter.
(14) If enrollment and binding are being done in person and cannot be completed in a single physical encounter, temporary secrets SHALL NOT be reused.
(15) If enrollment and binding are being done in person and cannot be completed in a single physical encounter and the CSP issues long-term authenticator secrets during a physical transaction, they SHALL be loaded locally onto a physical device that is issued in person to the applicant or delivered in a manner that confirms the address of record.
(16) Before adding a new authenticator to a subscriber's account, the CSP SHALL first require the subscriber to authenticate at AAL2 (or a higher AAL) at which the new authenticator will be used.
(17) If the subscriber's account has only one authentication factor bound to it, the CSP SHALL require the subscriber to authenticate at AAL1 to bind an additional authenticator of a different authentication factor.
(18) If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2, that subscriber SHALL repeat the identity proofing process described in IA-12.
(19) If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2 or IAL3, the CSP SHALL require the claimant to authenticate using an authenticator of the remaining factor, if any, to confirm binding to the existing identity.
(20) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then it requires entry of a confirmation code sent to an address of record.
(21) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL consist of at least 6 random alphanumeric characters generated by an approved random bit generator [SP 800-90Ar1].
(22) If the CSP opts to allow binding of a new memorized secret with the use of two physical authenticators, then the confirmation code SHALL be valid for a maximum of 7 days, but MAY be made valid up to 21 days via an exception process to accommodate addresses outside the direct reach of the U.S. Postal Service. Confirmation codes sent by means other than physical mail SHALL be valid for a maximum of 5 minutes.

o. Session Management: The following requirements apply to applications where a session is maintained between the subscriber and relying party to allow multiple interactions without repeating the authentication event each time.

Once an authentication event has taken place, it is often desirable to allow the subscriber to continue using the application across multiple subsequent interactions without requiring them to repeat the authentication event. This requirement is particularly true for federation scenarios where the authentication event necessarily involves several components and parties coordinating across a network.

(1) Session Binding Requirements: A session occurs between the software that a subscriber is running — such as a browser, application, or operating system (i.e., the session subject) — and the RP or CSP that the subscriber is accessing (i.e., the session host).

a. A session is maintained by a session secret which SHALL be shared between the subscriber's software and the service being accessed.

b. The secret SHALL be presented directly by the subscriber's software or possession of the secret SHALL be proven using a cryptographic mechanism.

c. The secret used for session binding SHALL be generated by the session host in direct response to an authentication event.

d. A session SHALL NOT be considered at a higher AAL than the authentication event.

e. Secrets used for session binding SHALL be generated by the session host during an interaction, typically immediately following authentication.

f. Secrets used for session binding SHALL be generated by an approved random bit generator [SP 800-90Ar1].

g. Secrets used for session binding SHALL contain at least 64 bits of entropy.

h. Secrets used for session binding SHALL be erased or invalidated by the session subject when the subscriber logs out.

i. Secrets used for session binding SHALL be sent to and received from the device using an authenticated protected channel.

j. Secrets used for session binding SHALL time out and not be accepted after the times specified in IA-5 j (13) as appropriate for the AAL.

k. Secrets used for session binding SHALL NOT be available to insecure communications between the host and subscriber's endpoint.

l. Authenticated sessions SHALL NOT fall back to an insecure transport, such as from https to http, following authentication.

m. URLs or POST content SHALL contain a session identifier that SHALL be verified by the RP to ensure that actions taken outside the session do not affect the protected session.

n. Browser cookies SHALL be tagged to be accessible only on secure (HTTPS) sessions.

o. Browser cookies SHALL be accessible to the minimum practical set of hostnames and paths.

p. Expiration of browser cookies SHALL NOT be depended upon to enforce session timeouts.

q. The presence of an OAuth access token SHALL NOT be interpreted by the RP as presence of the subscriber, in the absence of other signals.

(2) Reauthentication Requirements

a. Continuity of authenticated sessions SHALL be based upon the possession of a session secret issued by the verifier at the time of authentication and optionally refreshed during the session.

b. Session secrets SHALL be non-persistent, i.e., they SHALL NOT be retained across a restart of the associated application or a reboot of the host device.

c. Periodic reauthentication of sessions (at least every 12 hours per session) SHALL be performed to confirm the continued presence of the subscriber at an authenticated session.

d. A session SHALL NOT be extended past the guidelines in IA-5 o (2) a – j based on presentation of the session secret alone.

e. Prior to session expiration, the reauthentication time limit SHALL be extended by prompting the subscriber for the authentication factor(s) of a memorized secret or biometric.

f. If federated authentication is being used, then since the CSP and RP often employ separate session management technologies, there SHALL NOT be any assumption of correlation between these sessions.

g. An RP requiring reauthentication through a federation protocol SHALL — if possible within the protocol — specify the maximum (see IA-5 j (10)) acceptable authentication age to the CSP.

h. If federated authentication if being used and an RP has specific authentication age (see IA-5 j [10]) requirements that it has communicated to the CSP, then the CSP SHALL reauthenticate the subscriber if they have not been authenticated within that time period.
i. If federated authentication is being used, the CSP SHALL communicate the authentication event time to the RP to allow the RP to decide if the assertion is sufficient for reauthentication and to determine the time for the next reauthentication event.

(1) AUTHENTICATOR MANAGEMENT | AUTHENTICATOR TYPES

(a) Memorized Secret Authenticators and Verifiers

Current - These controls are currently sanctionable for audit.

Password-based authentication applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)(a)(5). The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof.

1. Maintain a list of commonly used, expected, or compromised passwords and update the list quarterly and when organizational passwords are suspected to have been compromised directly or indirectly.

Per Jeff Campbell (FBI Deputy ISO), the following basic password standards found in IA-5(1)(a)(5) will no longer be acceptable on October 1, 2024

5. Enforce the following composition and complexity rules when agencies elect to follow basic password standards:

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

6. If chosen by the subscriber, memorized secrets SHALL be at least 8 characters in length.
9. Memorized secret verifiers SHALL NOT permit the subscriber to store a “hint” that is accessible to an unauthenticated claimant.
11. When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly used, expected, or compromised.
17. The verifier SHALL use approved encryption when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.
18. The verifier SHALL use an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.
19. Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks.
20. Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function.
21. The salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.
22. Both the salt value and the resulting hash SHALL be stored for each subscriber using a memorized secret authenticator

10/01/2024 - These controls are not sanctionable for audit until October 1, 2024

2. Require immediate selection of a new password upon account recovery;
3. Allow user selection of long passwords and passphrases, including spaces and all printable characters;
4. Employ automated tools to assist the user in selecting strong password authenticators;

7. If chosen by the CSP or verifier using an approved random number generator, memorized secrets SHALL be at least 6 characters in length.
8. Truncation of the secret SHALL NOT be performed.
10. Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets.
12. If a chosen secret is found in the list, the CSP or verifier SHALL advise the subscriber that they need to select a different secret.
13. If a chosen secret is found in the list, the CSP or verifier SHALL provide the reason for rejection.
14. If a chosen secret is found in the list, the CSP or verifier SHALL require the subscriber to choose a different value.
15. Verifiers SHALL implement a rate-limiting mechanism that effectively limits failed authentication attempts that can be made on the subscriber's account to no more than five.
16. Verifiers SHALL force a change of memorized secret if there is evidence of compromise of the authenticator.
23. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be generated with an approved random bit generator and of sufficient length.
24. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL provide at least the minimum-security strength.
25. If an additional iteration of a key derivation function using a salt value known only to the verifier is performed, then this secret salt value SHALL be stored separately from the memorized secrets.

(b) Look-Up Secret Authenticators and Verifiers

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

1. CSPs creating look-up secret authenticators SHALL use an approved random bit generator to generate the list of secrets.
2. Look-up secrets SHALL have at least 20 bits of entropy.
3. If look-up secrets are distributed online, then they SHALL be distributed over a secure channel in accordance with the post-enrollment binding requirements in IA-5 'n' 17 through 25.
4. Verifiers of look-up secrets SHALL prompt the claimant for the next secret from their authenticator or for a specific (e.g., numbered) secret.
5. A given secret from an authenticator SHALL be used successfully only once.
6. If a look-up secret is derived from a grid (bingo) card, then each cell of the grid SHALL be used only once.
7. Verifiers SHALL store look-up secrets in a form that is resistant to offline attacks.
8. If look-up secrets have at least 112 bits of entropy, then they SHALL be hashed with an approved one-way function
9. If look-up secrets have less than 112 bits of entropy, then they SHALL be salted and hashed using a suitable one-way key derivation function.
10. If look-up secrets have less than 112 bits of entropy, then the salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.
11. If look-up secrets have less than 112 bits of entropy, then both the salt value and the resulting hash SHALL be stored for each look-up secret.
12. If look-up secrets that have less than 64 bits of entropy, then the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account.
13. The verifier SHALL use approved encryption when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.
14. The verifier SHALL use an authenticated protected channel when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.

(c) Out-of-Band Authenticators and Verifiers

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

1. The out-of-band authenticator SHALL establish a separate channel with the verifier in order to retrieve the out-of-band secret or authentication request.
2. Communication over the secondary channel SHALL be encrypted unless sent via the public switched telephone network (PSTN).
3. Methods that do not prove possession of a specific device, such as voice-over-IP (VoIP) or email, SHALL NOT be used for out-of-band authentication.
4. If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL uniquely authenticate itself by establishing an authenticated protected channel with the verifier.
5. If PSTN is not being used for out-of-band communication, then the out-of-band authenticator SHALL communicate with the verifier using approved cryptography.
6. If PSTN is not being used for out-of-band communication, then the key used to authenticate the out-of-band device SHALL be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, TEE, secure element).
7. If the PSTN is used for out-of-band authentication and a secret is sent to the out-of-band device via the PSTN, then the out-of-band authenticator SHALL uniquely authenticate itself to a mobile telephone network using a SIM card or equivalent that uniquely identifies the device.
8. If the out-of-band authenticator sends an approval message over the secondary communication channel, it SHALL either accept transfer of a secret from the primary channel to be sent to the verifier via the secondary communications channel, or present a secret received via the secondary channel from the verifier and prompt the claimant to verify the consistency of that secret with the primary channel, prior to accepting a yes/no response from the claimant which it sends to the verifier.
9. The verifier SHALL NOT store the identifying key itself, but SHALL use a verification method (e.g., an approved hash function or proof of possession of the identifying key) to uniquely identify the authenticator.
10. Depending on the type of out-of-band authenticator, one of the following SHALL take place: transfer of a secret to the primary channel, transfer of a secret to the secondary channel, or verification of secrets by the claimant.
11. If the out-of-band authenticator operates by transferring the secret to the primary channel, then the verifier SHALL transmit a random secret to the out-of-band authenticator and then wait for the secret to be returned on the primary communication channel.
12. If the out-of-band authenticator operates by transferring the secret to the secondary channel, then the verifier SHALL display a random authentication secret to the claimant via the primary channel and then wait for the secret to be returned on the secondary channel from the claimant's out-of-band authenticator.
13. If the out-of-band authenticator operates by verification of secrets by the claimant, then the verifier SHALL display a random authentication secret to the claimant via the primary channel, send the same secret to the out-of-band authenticator via the secondary channel for presentation to the claimant, and then wait for an approval (or disapproval) message via the secondary channel.
14. The authentication SHALL be considered invalid if not completed within 10 minutes.
15. Verifiers SHALL accept a given authentication secret only once during the validity period.
16. The verifier SHALL generate random authentication secrets with at least 20 bits of entropy.
17. The verifier SHALL generate random authentication secrets using an approved random bit generator.
18. If the authentication secret has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 l (3) through (4).

19. If out-of-band verification is to be made using the PSTN, then the verifier SHALL verify that the pre-registered telephone number being used is associated with a specific physical device.
20. If out-of-band verification is to be made using the PSTN, then changing the pre-registered telephone number is considered to be the binding of a new authenticator and SHALL only occur as described in IA-5 n (17) through (25).
21. If PSTN is used for out-of-band authentication, then the CSP SHALL offer subscribers at least one alternate authenticator that is not RESTRICTED and can be used to authenticate at the required AAL.
22. If PSTN is used for out-of-band authentication, then the CSP SHALL Provide meaningful notice to subscribers regarding the security risks of the RESTRICTED authenticator and availability of alternative(s) that are not RESTRICTED.
23. If PSTN is used for out-of-band authentication, then the CSP SHALL address any additional risk to subscribers in its risk assessment.
24. If PSTN is used for out-of-band authentication, then the CSP SHALL develop a migration plan for the possibility that the RESTRICTED authenticator is no longer acceptable at some point in the future and include this migration plan in its digital identity acceptance statement.

(d) OTP Authenticators and Verifiers

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

1. The secret key and its algorithm SHALL provide at least the minimum security strength of 112 bits as of the date of this publication.
2. The nonce SHALL be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.
3. OTP authenticators — particularly software-based OTP generators —SHALL NOT facilitate the cloning of the secret key onto multiple devices.
4. The authenticator output SHALL have at least 6 decimal digits (approximately 20 bits) of entropy.
5. If the nonce used to generate the authenticator output is based on a real-time clock, then the nonce SHALL be changed at least once every 2 minutes.
6. The OTP value associated with a given nonce SHALL be accepted only once.
7. The symmetric keys used by authenticators are also present in the verifier and SHALL be strongly protected against compromise.
8. If a single-factor OTP authenticator is being associated with a subscriber account, then the verifier or associated CSP SHALL use approved cryptography to either generate and exchange or to obtain the secrets required to duplicate the authenticator output.
9. The verifier SHALL use approved encryption when collecting the OTP.
10. The verifier SHALL use an authenticated protected channel when collecting the OTP.
11. If a time-based OTP is used, it SHALL have a defined lifetime (recommended 30 seconds) that is determined by the expected clock drift — in either direction — of the authenticator over its lifetime, plus allowance for network delay and user entry of the OTP.
12. Verifiers SHALL accept a given time-based OTP only once during the validity period.
13. If the authenticator output has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in IA-5 l (3) through (4).
14. If the authenticator is multi-factor, then each use of the authenticator SHALL require the input of the additional factor.
15. If the authenticator is multi-factor and a memorized secret is used by the authenticator for activation, then that memorized secret SHALL be a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of IA-5 (1)(a).
16. If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in IA-5 l (3) through (4).
17. If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures.

18. If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an OTP has been generated.
19. If the authenticator is multi-factor, the verifier or CSP SHALL establish, via the authenticator source, that the authenticator is a multi-factor device.
20. In the absence of a trusted statement that it is a multi-factor device, the verifier SHALL treat the authenticator as single-factor, in accordance with IA-5 (1) (d) (1) through (13).

(e) Cryptographic Authenticators and Verifiers (including single- and multi-factor cryptographic authenticators, both hardware- and software-based)

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

1. If the cryptographic authenticator is software based, the key SHALL be stored in suitably secure storage available to the authenticator application.
2. If the cryptographic authenticator is software based, the key SHALL be strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access.
3. If the cryptographic authenticator is software based, it SHALL NOT facilitate the cloning of the secret key onto multiple devices.
4. If the authenticator is single-factor and hardware-based, secret keys unique to the device SHALL NOT be exportable (i.e., cannot be removed from the device).
5. If the authenticator is hardware-based, the secret key and its algorithm SHALL provide at least the minimum-security length of 112 bits as of the date of this publication.
6. If the authenticator is hardware-based, the challenge nonce SHALL be at least 64 bits in length.
7. If the authenticator is hardware-based, approved cryptography SHALL be used.
8. Cryptographic keys stored by the verifier SHALL be protected against modification.
9. If symmetric keys are used, cryptographic keys stored by the verifier SHALL be protected against disclosure.
10. The challenge nonce SHALL be at least 64 bits in length.
11. The challenge nonce SHALL either be unique over the authenticator's lifetime or statistically unique (i.e., generated using an approved random bit generator).
12. The verification operation SHALL use approved cryptography.
13. If a multi-factor cryptographic software authenticator is being used, then each authentication requires the presentation of the activation factor.
14. If the authenticator is multi-factor, then any memorized secret used by the authenticator for activation SHALL be a randomly chosen numeric secret at least 6 decimal digits in length or other memorized secret meeting the requirements of IA-5 (1) (a).
15. If the authenticator is multi-factor, then use of a memorized secret for activation SHALL be rate limited as specified in IA-5 l (3) through (4).
16. If the authenticator is multi-factor and is activated by a biometric factor, then that factor SHALL meet the requirements of IA-5 m, including limits on the number of consecutive authentication failures.
17. If the authenticator is multi-factor, then the unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an authentication transaction has taken place.

(2) AUTHENTICATOR MANAGEMENT | PUBLIC KEY BASED AUTHENTICATION

Current - The control is currently sanctionable for audit.

For public key-based authentication, enforce authorized access to the corresponding private key and

map the authenticated identity to the account of the individual or group, and when public key infrastructure (PKI) is used, validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information, and implement a local cache of revocation data to support path discovery and validation.

(6) AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS

Current - The control is currently sanctionable for audit.

Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

IA-6 AUTHENTICATION FEEDBACK

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

Authentication feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems, such as desktops or notebooks with relatively large monitors, the threat (referred to as shoulder surfing) may be significant.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

Non-organizational users include system users other than organizational users explicitly covered by IA-2. Non-organizational users are uniquely identified and authenticated for accesses other than those explicitly identified and documented in AC-14. Identification and authentication of non-organizational users accessing federal systems may be required to protect federal, proprietary, or privacy-related information.

(1) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

Accept and electronically verify Personal Identity Verification-compliant credentials from other federal, state, local, tribal, or territorial (SLTT) agencies.

(2) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF EXTERNAL AUTHENTICATORS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

Accept only external authenticators that are NIST-compliant and Document and maintain a list of accepted external authenticators.

Acceptance of only NIST-compliant external authenticators applies to organizational systems that are accessible to the public (e.g., public-facing websites). External authenticators are issued by nonfederal government entities and are compliant with the CJISSECPOL. Approved external authenticators meet or

exceed the minimum Federal Government-wide technical, security, privacy, and organizational maturity requirements.

(4) IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF DEFINED PROFILES

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

Conform to the following profiles for identity management: Security Assertion Markup Language (SAML) or OpenID Connect.

Organizations define profiles for identity management based on open identity management standards.

IA-11 RE-AUTHENTICATION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency must require users to re-authenticate when: roles, authenticators, or credentials change, security categories of systems change, the execution of privileged functions occur, or every 12 hours.

NOTE: This needs to be coordinated if you have personnel on duty more than 12 hours. I highly suggest the agency establish policy to prevent someone being logged out during a critical event, such as a 911 call. Remember, everyone, even Dispatch and the Mobile Units must log out and log back in at least once every twelve hours. Please consider this in mobile command units if a computer, with access to CJI, is in use during the call, especially if the terminal is in use while conducting suspect negotiations.
We have had request for an exception in both Dispatch and in the Patrol Units and they have been denied. If you have a specific request for an exception, please submit the request to the CJIS Security Office at security.committee@dps.texas.gov and describe the situation in detail.

IA-12 IDENTITY PROOFING

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

NOTE: The agency will likely need skilled IT resources to be able to meet this requirement.

The agency is required to identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines. Resolve user identities to a unique individual and collect, validate, and verify identity evidence.

Identity proofing is the process of collecting, validating, and verifying a user's identity information for the purposes of establishing credentials for accessing a system. Identity proofing is intended to mitigate threats to the registration of users and the establishment of their accounts.

(2) IDENTITY PROOFING | IDENTITY EVIDENCE

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

Require evidence of individual identification be presented to the registration authority.

Identity evidence, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity or at least increases the work factor of potential adversaries.

(3) IDENTITY PROOFING | IDENTITY EVIDENCE VALIDATION AND VERIFICATION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

a. Require that the presented identity evidence be validated and verified through agency-defined resolution, validation, and verification methods.

b. Identity proofing SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits.

c. 1. Collection of PII SHALL be limited to the minimum necessary to resolve to a unique identity in a given context.

2. Collection of PII SHALL be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the applicant providing identity evidence for appropriate identity resolution, validation, and verification.

d. The CSP SHALL provide explicit notice to the applicant at the time of collection regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes.
e. If CSPs process attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, or to comply with law or legal process, then CSPs SHALL implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing.
f. If the CSP employs consent as part of its measures to maintain predictability and manageability, …then it SHALL NOT make consent for the additional processing a condition of the identity service.
g. The CSP SHALL provide mechanisms for redress of applicant complaints or problems arising from the identity proofing.
h. The CSP SHALL assess the [redress] mechanisms for their efficacy in achieving resolution of complaints or problems.
i. The identity proofing and enrollment processes SHALL be performed according to an applicable written policy or *practice statement* that specifies the particular steps taken to verify identities.
j. The *practice statement* SHALL include control information detailing how the CSP handles proofing errors that result in an applicant not being successfully enrolled.
k. The CSP SHALL maintain a record, including audit logs, of all steps taken to verify the identity of the applicant as long as the identity exists in the information system.
l. The CSP SHALL record the types of identity evidence presented in the proofing process.
m. The CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine:

1. Any steps that it will take to verify the identity of the applicant beyond any mandatory requirements specified herein;
2. The PII, including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing (Note: Specific federal requirements may apply); and
3. The schedule of retention for these records (Note: CSPs may be subject to specific retention policies in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply).

n. All PII collected as part of the enrollment process SHALL be protected to ensure confidentiality, integrity, and attribution of the information source.
o. "The entire proofing transaction, including transactions that involve a third party, SHALL occur over authenticated protected channels. "
*TLS version 1.2 or greater is recommended.
p. If the CSP uses fraud mitigation measures, then the CSP SHALL conduct a privacy risk assessment for these mitigation measures.
Such assessments SHALL include any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography), and be documented per requirement IA-12(3) k – m above.
q. In the event a CSP ceases to conduct identity proofing and enrollment processes, then the CSP SHALL be responsible for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention.
r. Regardless of whether the CSP is a federal agency or non-federal entity, the following requirements apply to the federal agency offering or using the proofing service:

1. The agency SHALL consult with their Senior Agency Official for Privacy (SAOP) to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers Privacy Act requirements.
2. The agency SHALL publish a System of Records Notice (SORN) to cover such collection, as applicable.
3. The agency SHALL consult with their SAOP to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers E-Government Act of 2002 requirements.

4. The agency SHALL publish a Privacy Impact Assessment (PIA) to cover such collection, as applicable.

s. An enrollment code SHALL be comprised of one of the following:

1 Minimally, a random six character alphanumeric or equivalent entropy. For example, a code generated using an approved random number generator or a serial number for a physical hardware authenticator; OR

2 A machine-readable optical label, such as a QR Code, that contains data of similar or higher entropy as a random six character alphanumeric.

t. Training requirements for personnel validating evidence SHALL be based on the policies, guidelines, or requirements of the CSP or RP.

u. This criterion applies to CSPs that provide identity proofing and enrollment services to minors (under the age of 18):

v. The CSP SHALL have the operator view the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process.

w. The CSP SHALL collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject. All biometric performance requirements in IA-5 m (1) through (12) apply.

x. The CSP SHALL support in-person or remote identity proofing, or both.

y. The CSP SHALL collect the following from the applicant:

1. One piece of SUPERIOR or STRONG evidence if the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence and the CSP validates the evidence directly with the issuing source; OR

2. Two pieces of STRONG evidence; OR

3. One piece of STRONG evidence plus two pieces of FAIR evidence

z. The CSP SHALL validate each piece of evidence with a process that can achieve the same strength as the evidence presented (see 'y' above). For example, if two forms of STRONG identity evidence are presented, each piece of evidence will be validated at a strength of STRONG.

aa. The CSP SHALL verify identity evidence as follows:

At a minimum, the applicant's binding to identity evidence must be verified by a process that is able to achieve a strength of STRONG.

bb. For IAL2 remote proofing: The collection of biometric characteristics for physical or biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity performed remotely SHALL adhere to all requirements as specified in IA-5 m.

cc. Knowledge-based verification (KBV) SHALL NOT be used for in-person (physical or supervised remote) identity verification.

dd. The CSP SHALL employ appropriately tailored security controls, to include control enhancements, from the moderate or high baseline of security controls defined in the CJISSECPOL.

ee. Supervised Remote Identity Proofing: Supervised remote identity proofing is intended to provide controls for comparable levels of confidence and security to in-person IAL3 identity proofing for identity proofing processes that are performed remotely. Supervised remote identity proofing is optional for CSPs; that is, if a CSP chooses to use supervised remote identity proofing, then the following requirements, (1) through (8), would apply. It should be noted that the term "supervised remote identity proofing" has specialized meaning and is used only to refer to the specialized equipment and the following control requirements, (1) through (8). In addition to those requirements presented in this document, as well as the applicable identity validation and verification requirements, CSPs that provide supervised remote identity proofing services must demonstrate conformance with the requirements contained in this section. The following requirements for supervised remote proofing apply specifically to IAL3. If the equipment/facilities used for supervised remote proofing are used for IAL2 identity proofing, the following requirements, (1) through (8), for supervised remote proofing do not apply. In this case, the requirements for conventional remote identity proofing are applicable.

1. Supervised remote identity proofing and enrollment transactions SHALL meet the following requirements, in addition to the IAL3 validation and verification requirements specified in IA-12(3)s.
2. The CSP SHALL monitor the entire identity proofing session, from which the applicant SHALL NOT depart — for example, by a continuous high-resolution video transmission of the applicant.
3. The CSP SHALL have a live operator participate remotely with the applicant for the entirety of the identity proofing session.
4. The CSP SHALL require all actions taken by the applicant during the identity proofing session to be clearly visible to the remote operator.
5. The CSP SHALL require that all digital validation of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors.
6. The CSP SHALL require operators to have undergone a training program to detect potential fraud and to properly perform a supervised remote proofing session.
7. The CSP SHALL employ physical tamper detection and resistance features appropriate for the environment in which it is located.
8. The CSP SHALL ensure that all communications occur over a mutually authenticated protected channel.

ff. Trusted Referee: The use of trusted referees is optional for CSPs; that is, if a CSP chooses to use trusted referees for identity proofing and enrollment, then the following requirements, (1) through (3), would apply. The use of trusted referees is intended to assist in the identity proofing and enrollment for populations that are unable to meet IAL2 identity proofing requirements, or otherwise would be challenged to perform identity proofing and enrollment process requirements. Such populations may include, but are not limited to:

- disabled individuals;
- elderly individuals;
- homeless individuals,
- individuals with little or no access to online services or computing devices;
- unbanked and individuals with little or no credit history;
- victims of identity theft;
- children under 18; and
- immigrants.

In addition to those requirements presented in the General section of this document, as well as the applicable IAL requirements, CSPs that use trusted referees in their identity proofing services must demonstrate conformance with the requirements contained in this section.
1. If the CSP uses trusted referees, then…The CSP SHALL establish written policy and procedures as to how a trusted referee is determined and the lifecycle by which the trusted referee retains their status as a valid referee, to include any restrictions, as well as any revocation and suspension requirements.
2. If the CSP uses trusted referees, then…The CSP SHALL proof the trusted referee at the same IAL as the applicant proofing.
3. If the CSP uses trusted referees, then…The CSP SHALL determine the minimum evidence required to bind the relationship between the trusted referee and the applicant.

(5) IDENTITY PROOFING | ADDRESS CONFIRMATION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

a. Require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record.
b. The CSP SHALL confirm address of record.
c. Valid records to confirm address SHALL be issuing source(s) or authoritative source(s).
d. Note that IAL2-7 applies only to in-person proofing at IAL2.
If the CSP performs in-person proofing for IAL2 and provides an enrollment code directly to the subscriber for binding to an authenticator at a later time, then the enrollment code…SHALL be valid for a maximum of seven (7) days.
e. For remote identity proofing at IAL2:

The CSP SHALL send an enrollment code to a confirmed address of record for the applicant.
f. For remote identity proofing at IAL2:
The applicant SHALL present a valid enrollment code to complete the identity proofing process.
g. Note that the following enrollment code validity periods apply to enrollment codes sent to confirmed addresses of record for IAL2 remote in-person proofing only.
Enrollment codes shall have the following maximum validities:

1. 10 days, when sent to a postal address of record within the contiguous United States;
2. 30 days, when sent to a postal address of record outside the contiguous United States;
3. 10 minutes, when sent to a telephone of record (SMS or voice);
4. 24 hours, when sent to an email address of record.

h. If the enrollment code sent to the confirmed address of record as part of the remote identity proofing process at IAL2 is also intended to be an authentication factor, then…it SHALL be reset upon first use.
i. If the CSP performs remote proofing at IAL2 and optionally sends notification of proofing in addition to sending the required enrollment code, then…The CSP SHALL ensure the enrollment code and notification of proofing are sent to different addresses of record.

5.14 SYSTEM AND SERVICES ACQUISITION (SA)

SA-22 UNSUPPORTED SYSTEM COMPONENTS

Current - The control is currently sanctionable for audit.
NOTE: The agency will likely need skilled IT resources to be able to meet this requirement.

Previously, the State of Texas Security Policy Supplement required all IT systems with CJIS connectivity shall be replaced within six (6) months of becoming "End-of-Life", or no longer supported by the manufacturer with security hot fixes, updates, and patches.

The current CJISSECPOL requires agencies to replace system components when support for the components is no longer available (End-of-Support) from the developer, vendor, or manufacturer or provide the following options for alternative sources for continued support for unsupported components: original manufacturer support, or original contracted vendor support. So, the CJISSECPOL removes the risks associated with running unsupported systems for up to six (6) months after the device reaches End-of-Support.

Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option. The increased risk of using unsupported system components can be mitigated, for example, by prohibiting the connection of such components to public or uncontrolled networks or implementing other forms of isolation. This is an option for legacy RMS systems the agency wants to retain, assuming the vendor allows them to do so. DPS will be assessing the isolation of such systems and they must be disclosed during audits and represented on the agency network diagram.

In addition, DPS will be requesting an agency equipment list, along with a current agency network diagram, that should list all managed equipment used to process, store, or transmit CJI. All this equipment should be represented on the agency network diagram. The equipment list shall include the Make, Model, Current O/S and/or Firmware Version, Date it was last updated, End of Support Date. This list shall be maintained by the agency and kept current along with the agency network diagram and made available upon request by DPS for audits, changes, etc. This is also a good reference for the agency to be able to plan and budget for equipment upgrades.

NOTE: The End-of-Support date is not the same as the End-of-Life or End-of-Sale date.

For example:

CISCO 2010 Connected Grid Router

Status: End of Sale (EOL Details)
Release Date: 24-MAY-2010
End-of-Sale Date: 01-MAR-2023
End-of-Support Date: 29-FEB-2028

5.15 SYSTEM AND INFORMATION INTEGRITY (SI)

SI-1 POLICY AND PROCEDURES

Current - The control is currently sanctionable for audit.

This is where the agency establishes and documents agency policy, including Purpose, Scope, Roles, Responsibilities, Management Commitment, Coordination among agency entities, Compliance and step by step procedures as to how the policy will be implemented at the agency.

The agency must designate an individual with security responsibilities to manage the development, documentation, and dissemination of the agency policies and procedures, and review and update the policy annually, and after any security incidents.

SI-2 FLAW REMEDIATION

Current - The control is currently sanctionable for audit.

NOTE: The agency will need skilled IT resources to be able to meet this requirement.

Previously, the State of Texas Security Policy Supplement required all components of IT systems with CJIS connectivity shall be updated with all available Security Hot fixes, updates, and patches within 30 days of availability. This applied to workstations, servers, laptops, switches, routers, and all other managed IT equipment.

The current CJISSECPOL requires agencies to identify, report, and correct system flaws. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation and install security-relevant software and firmware updates within the number of days listed after the release of the updates:

- Critical – 15 days
- High – 30 days
- Medium – 60 days
- Low – 90 days

and incorporate flaw remediation into the organizational configuration management process.

This may be challenging for many agencies that have isolated TLETS terminals that are only connected to the DPS Satellite. The satellites are in the process of being replaced with DPS provided and monitored routers which will connect through the agency Internet Service Provider (ISP), unless the agency has a dedicated circuit to DPS.

Please do not connect the TLETS terminals to the agency network unless they are protected by a firewall. If you have any questions regarding moving TLETS terminals, please contact the CJIS Security Office at (512) 424.5686 PRIOR to making the change.

The time required to download, test, and schedule installation, in addition to the potential downtime associated with applying these updates is expected to put quite a workload on agency IT Support resources.

(2) FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS

Current - The control is currently sanctionable for audit.

Determine if system components have applicable security-relevant software and firmware updates installed using vulnerability scanning tools as least quarterly or following any security incidents involving CJI or systems used to process, store, or transmit CJI.

SI-3 MALICIOUS CODE PROTECTION

Current- The control is currently sanctionable for audit.

NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to Implement signature-based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.

Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures.

Configure malicious code protection mechanisms to:

1. Perform periodic scans of the system at least daily and real-time scans of files from external sources at network entry and exit points and on all servers and endpoint devices as the files are downloaded, opened, or executed in accordance with organizational policy.

2. Block or quarantine malicious code, take mitigating action(s), and when necessary, implement incident response procedures; and send alert to system/network administrators and/or organizational personnel with information security responsibilities in response to malicious code detection.

Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

SI-4 SYSTEM MONITORING

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to monitor the system to detect:

1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives:
    a. Intrusion detection and prevention.
    b. Malicious code protection.
    c. Vulnerability scanning.
    d. Audit record monitoring.
    e. Network monitoring.
    f. Firewall monitoring.
2. Unauthorized local, network, and remote connections
    b. Identify unauthorized use of the system through event logging.
    c. Invoke internal monitoring capabilities or deploy monitoring devices:
        1. Strategically within the system to collect organization-determined essential information; and
        2. At ad hoc locations within the system to track specific types of transactions of interest to the organization.
    d. Analyze detected events and anomalies.
    e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation.
    f. Obtain legal opinion regarding system monitoring activities.
    g. Provide intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring, and firewall monitoring software logs to organizational personnel with information security responsibilities weekly.

(2) SYSTEM MONITORING | AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

Employ automated tools and mechanisms to support near real-time analysis of events.

Automated tools and mechanisms include host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or security information and event management (SIEM) technologies that provide real-time analysis of alerts and notifications generated by organizational systems.

(4) SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic.

Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions such as: the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information (e.g.: egress monitoring).

(5) SYSTEM MONITORING | SYSTEM-GENERATED ALERTS

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to alert organizational personnel with system monitoring responsibilities when the following system-generated indications of compromise or potential compromise occur, including inappropriate or unusual activities with security or privacy implications.

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to receive system security alerts, advisories, and directives from external source(s): e.g.:

CISA - https://public.govdelivery.com/accounts/USDHSCISA/subscriber/new?qsp=CODE_RED

Multi-State Information Sharing & Analysis Center [MS-ISAC] - https://www.cisecurity.org/cybersecurity-threats

U.S. Computer Emergency Readiness Team [USCERT]- integrated with CISA (above)

and hardware/software providers, federal/state advisories, etc. on an ongoing basis.

Generate internal security alerts, advisories, and directives as deemed necessary.

Disseminate security alerts, advisories, and directives to organizational personnel implementing, operating, maintaining, and using the systems.

Implement security directives in accordance with established time frames or notify the issuing organization of the degree of noncompliance.

To do so, the agency will need to subscribe to receive alerts, advisories, and directives from the agency hardware/software vendors on an ongoing basis. More importantly, the agency will need skilled IT Resources that can understand the content of these alerts, advisories, and directives.

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
These unauthorized changes need to be reported to DPS using the agency Incident Response procedures, per SI-7(7) below.

The agency is required to employ integrity verification tools to detect unauthorized changes to software, firmware, and information systems that contain or process CJI and when unauthorized changes to the software, firmware, and information are detected, notify organizational personnel responsible for software, firmware, and/or information integrity and implement incident response procedures as appropriate.

Integrity-checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications.

(1) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to perform an integrity check of software, firmware, and information systems that contain or process CJI at agency-defined transitional states or security relevant events at least weekly or in an automated fashion.

Security-relevant events include the identification of new threats to which organizational systems are susceptible and the installation of new hardware, software, or firmware.

Transitional states include system startup, restart, shutdown, and abort.

(7) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to incorporate the detection of the following unauthorized changes into the organizational incident response capability: unauthorized changes to established configuration setting or the unauthorized elevation of system privileges.

SI-8 SPAM PROTECTION

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages and update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

I would not be surprised to hear that this security control has been in the CJIS Security Policy since version 1.0.

(2) SPAM PROTECTION | AUTOMATIC UPDATES

Current - The control is currently sanctionable for audit.

NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Automatically update spam protection mechanisms at least daily.

This may be challenging for many agencies that have isolated TLETS terminals that are only connected to the DPS Satellite. The satellites are in the process of being replaced with DPS provided and monitored routers which will connect through the agency Internet Service Provider (ISP), unless the agency has a dedicated circuit to DPS. Please do not connect the TLETS terminals to the agency network unless they are protected by a firewall. If you have any questions regarding moving TLETS terminals, please contact the CJIS Security Office at (512) 424.5686 PRIOR to making the change.

SI-10 INFORMATION INPUT VALIDATION

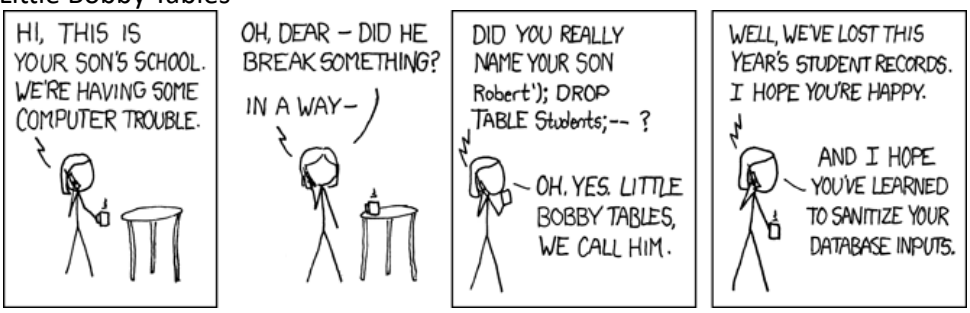
Current - The control is currently sanctionable for audit.

NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Check the validity of the following information inputs: all inputs to web/application servers, database servers, and any system or application input that might receive or process CJI.

For example: A SQL Injection:

Little Bobby Tables



SI-11 ERROR HANDLING

Current - The control is currently sanctionable for audit.

NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to ensure error messages only provide information necessary for corrective actions without revealing information that could be exploited and reveal error messages only to organizational personnel with information security responsibilities.

The agency should review this with agency selected vendor solutions and identify the appropriate agency personnel that will review the error messages, especially if the error messages are presented to the public.

SI-12 INFORMATION MANAGEMENT AND RETENTION

Current - The control is currently sanctionable for audit.

The agency will need to manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements.

(1) INFORMATION MANAGEMENT AND RETENTION | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

Current - The control is currently sanctionable for audit.

Limit personally identifiable information being processed in the information life cycle to the minimum PII necessary to achieve the purpose for which it is collected.

Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining which elements of personally identifiable information may create risk.

(2) INFORMATION MANAGEMENT AND RETENTION | MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency should be using data obfuscation, randomization, anonymization techniques, or use synthetic data to minimize the use of personally identifiable information for research, testing, or training.

Think about this when a vendor asks for a dump of your agency old RMS data so they can develop data migration scripts to move your agency data to a new RMS solution. Especially, if the vendor is using offshore resources.

Does the agency really want the vendor to have a dump of all your RMS data?

Does the agency have a data sharing agreement in place to ensure the data does not end up on the Dark Web?

Per Wikipedia:

Data masking or data obfuscation is the process of modifying sensitive data in such a way that it is of no or little value to unauthorized intruders while still being usable by software or authorized personnel. Data masking can also be referred as anonymization, or tokenization, depending on different context.

(3) INFORMATION MANAGEMENT AND RETENTION | INFORMATION DISPOSAL

Current - The control is currently sanctionable for audit.

Use the following techniques to dispose of, destroy, or erase information following the retention period: as defined in MP-6 MEDIA SANITIZATION.

SI-16 MEMORY PROTECTION

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to implement data execution prevention and address space layout randomization to protect the system memory from unauthorized code execution.

Per Wikipedia:

In computer security, executable-space protection (Redirected Data Execution Prevention) marks memory regions as non-executable, such that an attempt to execute machine code in these regions will cause an exception.

Address space layout randomization (ASLR) is a computer security technique involved in preventing exploitation of memory corruption vulnerabilities.

CJISSECPOL v5.9.3

The FBI officially released CJISSECPOL version 5.9.3 September 14, 2023. This release was limited to the Incident Response, Access Control, and Maintenance security controls. Specifically,

- 5.3 INCIDENT RESPONSE (IR)
  - IR-1 POLICY AND PROCEDURES
  - IR-2 INCIDENT RESPONSE TRAINING
    - (3) INCIDENT RESPONSE TRAINING | BREACH
  - IR-3 INCIDENT RESPONSE TESTING
    - (2) INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS
  - IR-4 INCIDENT HANDLING
    - (1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES
  - IR-5 INCIDENT MONITORING
  - IR-6 INCIDENT REPORTING
    - (1) INCIDENT REPORTING | AUTOMATED REPORTING
    - (3) INCIDENT REPORTING | SUPPLY CHAIN COORDINATION
  - IR-7 INCIDENT RESPONSE ASSISTANCE
    - (1) INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT
  - IR-8 INCIDENT RESPONSE PLAN
    - (1) INCIDENT RESPONSE PLAN | BREACHES
- 5.5 ACCESS CONTROL (AC)
  - AC-1 POLICY AND PROCEDURES
  - AC-2 ACCOUNT MANAGEMENT
    - (1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT
    - (2) ACCOUNT MANAGEMENT | AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT
    - (3) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS
    - (4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS
    - (5) ACCOUNT MANAGEMENT | INACTIVITY LOGOUT
    - (13) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS
  - AC-3 ACCESS ENFORCEMENT
    - (14) ACCESS ENFORCEMENT | INDIVIDUAL ACCESS
  - AC-4 INFORMATION FLOW ENFORCEMENT
  - AC-5 SEPARATION OF DUTIES
  - AC-6 LEAST PRIVILEGE
    - (1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS
    - (2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS
    - (5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS
    - (7) LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES
    - (9) LEAST PRIVILEGE | LOG USE OF PRIVILEGED FUNCTIONS
    - (10) LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS
  - AC-7 UNSUCCESSFUL LOGON ATTEMPTS
  - AC-8 SYSTEM USE NOTIFICATION
  - AC-11 DEVICE LOCK
    - (1) DEVICE LOCK | PATTERN-HIDING DISPLAYS
  - AC-12 SESSION TERMINATION
  - AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
  - AC-17 REMOTE ACCESS
    - (1) REMOTE ACCESS | MONITORING AND CONTROL
    - (2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION
    - (3) REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS

5.3 INCIDENT RESPONSE (IR)

IR-1 POLICY AND PROCEDURES

Mixed - This control is currently sanctionable, except the annual review and update process which is not sanctionable for audit until October 1, 2024.

This is where the agency establishes and documents agency policy, including Purpose, Scope, Roles, Responsibilities, Management Commitment, Coordination among agency entities, Compliance and step by step procedures as to how the policy will be implemented at the agency.

The agency must designate an individual with security responsibilities to manage the development, documentation, and dissemination of the agency policies and procedures, and review and update the policy annually, and after any security incidents.

IR-2 INCIDENT RESPONSE TRAINING

Mixed - This control is currently sanctionable, except the annual review and update process which is not sanctionable for audit until October 1, 2024.

NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to provide incident response training to system users consistent with assigned roles and responsibilities prior to assuming an incident response role or responsibility or acquiring system access, when required by system changes and annually thereafter.

Review and update incident response training content annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

For example, users may only need to know who to call or how to recognize an incident; system administrators may require additional training on how to handle incidents; and incident responders may receive more specific training on forensics, data collection techniques, reporting, system recovery, and system restoration.

(3) INCIDENT RESPONSE TRAINING | BREACH

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.

IR-3 INCIDENT RESPONSE TESTING

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to test the effectiveness of the incident response capability for the system annually using the following tests: tabletop or walk-through exercises; simulations; or other agency-appropriate tests.

(2) INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Coordinate incident response testing with organizational elements responsible for related plans.

IR-4 INCIDENT HANDLING

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery. Coordinate incident handling activities with contingency planning activities. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly and ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

(1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Support the incident handling process using automated mechanisms (e.g., online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.

IR-5 INCIDENT MONITORING

Current - The control is currently sanctionable for audit.

Track and document incidents.

IR-6 INCIDENT REPORTING

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

Require personnel to report suspected incidents to the organizational incident response capability within immediately but not to exceed one (1) hour after discovery and report incident information to organizational personnel with incident handling responsibilities, and if confirmed, notify the CSO, SIB Chief, or Interface Agency Official.

The agency is required to notify DPS with one (1) hour after discovery by contacting the Operations Information Center (OIC) at (888) 377-6420.

Upon notification to the OIC, the Security Committee will contact the agency, determine if the agency needs any assistance from DPS Cyber Security, and request the Incident Response Form be submitted to DPS when there is confidence the agency email system is not compromised, or infected. DPS will also submit an online Incident Response form within the Technical Audit Portal, for DPS tracking purposes. The online form should be completed when things settle down and the agency is technically able to do so.

The agency should seriously consider disconnections and/or notifications to agencies that are interconnected, such as an agency that is hosted, or hosting other agencies, to prevent the potential

spread of the incident. DPS will make these determinations as needed to protect the potential spread to other agencies and/or the State.

(1) INCIDENT REPORTING | AUTOMATED REPORTING

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
Report incidents using automated mechanisms, which includes email.
PLEASE DO NOT WAIT TO SEE IF THE AGENCY CAN RESOLVE THE INCIDENT BEFORE REPORTING IT TO DPS.

(3) INCIDENT REPORTING | SUPPLY CHAIN COORDINATION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.
The agency determines the appropriate information to share and consider the value gained from informing external organizations about supply chain incidents, including the ability to improve processes or to identify the root cause of an incident.

IR-7 INCIDENT RESPONSE ASSISTANCE

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

DPS Cyber Security has resources that can be made available, at no cost to the agency, so please inform the Security Committee if assistance is requested so the appropriate resources can get in route to the agency.

(1) INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to increase the availability of incident response information and support using automated mechanisms described in the discussion.
Discussion: Automated mechanisms can provide a push or pull capability for users to obtain incident response assistance. For example, individuals may have access to a website to query the assistance capability, or the assistance capability can proactively send incident response information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support. If the automated mechanisms include external assistance that will give unescorted physical or logical access to CJI, it is imperative to ensure that the appropriate controls/procedures (CJIS Security Addendum/Outsourcing Standard) are in place. Examples would include Cyber Incident Response Vendors (IT Security/Law Firms).

IR-8 INCIDENT RESPONSE PLAN

Remember: Not having a plan, is a plan, for failure…
Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
The agency is required to:
Develop an incident response plan that:

- Provides the organization with a roadmap for implementing its incident response capability.
- Describes the structure and organization of the incident response capability.

Provides a high-level approach for how the incident response capability fits into the overall organization.
Meets the unique requirements of the organization, which relate to mission, size, structure, and functions.
Defines reportable incidents.
Provides metrics for measuring the incident response capability within the organization.
Defines the resources and management support needed to effectively maintain and mature an incident response capability.
Addresses the sharing of incident information.
Is reviewed and approved by the organization's/agency's executive leadership annually; and
Explicitly designates responsibility for incident response to organizational personnel with incident reporting responsibilities and CSO or CJIS WAN Official.

Distribute copies of the incident response plan to organizational personnel with incident handling responsibilities.
Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing.
Communicate incident response plan changes to organizational personnel with incident handling responsibilities.
Protect the incident response plan from unauthorized disclosure and modification.

(1) INCIDENT RESPONSE PLAN | BREACHES

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
Include in the Incident Response Plan for breaches involving personally identifiable information a process to determine if notice to individuals or other organizations, including oversight organizations, is needed, an assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms, and identification of applicable privacy requirements.

5.5 ACCESS CONTROL (AC)

AC-1 POLICY AND PROCEDURES

Mixed - This control is currently sanctionable, except the annual review and update process which is not sanctionable for audit until October 1, 2024.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
This is where the agency establishes and documents agency policy, including Purpose, Scope, Roles, Responsibilities, Management Commitment, Coordination among agency entities, Compliance and step by step procedures as to how the policy will be implemented at the agency.

The agency must designate an individual with security responsibilities to manage the development, documentation, and dissemination of the agency policies and procedures, and review and update the policy annually, and after any security incidents.

AC-2 ACCOUNT MANAGEMENT

Mixed - This control is a mixture of currently sanctionable controls and controls not sanctionable until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to define and document the types of accounts allowed and specifically prohibited for use within the system.
Assign account managers.
Require conditions for group and role membership.
Specify:

Authorized users of the system.
Group and role membership.
Access authorizations (i.e., privileges) and attributes listed below for each account.

Email Address text

Employer Name
Federation ID
Given Name
Identity Provider ID
Sur Name
Telephone Number
Unique Subject ID
Counter Terrorism Data Self Search Home Privilege Indicator
Criminal History Data Self Search Home Privilege Indicator
Criminal Intelligence Data Self Search Home Privilege Indicator
Criminal Investigative Data Self Search Home Privilege Indicator
Display Name
Government Data Self Search Home Privilege Indicator
Local ID
NCIC Certification Indicator
N-Dex Privilege Indicator
PCII Certification Indicator
Employer ORI
Employer Organization General Category Code
Employer State Code
Public Safety Officer Indicator
Sworn Law Enforcement Officer Indicator
Authenticator Assurance Level
Federation Assurance Level
Identity Assurance Level
Intelligence Analyst Indicator

Require approvals by organizational personnel with account management responsibilities for requests to create accounts.
Create, enable, modify, disable, and remove accounts in accordance with agency policy.
Monitor the use of accounts.
Notify account managers and system/network administrators within:

- One day when accounts are no longer required.
- One day when users are terminated or transferred.
- One day when system usage or need-to-know changes for an individual.

Authorize access to the system based on:
A valid access authorization.
Intended system usage.
Attributes as listed above.
Review accounts for compliance with account management requirements at least annually.
Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group.
Align account management processes with personnel termination and transfer processes.
The agency will want to refer to the Discussion section for this security control within the CJISECPOL.

(1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
Support the management of system accounts using automated mechanisms including email, phone, and text notifications.

(2) ACCOUNT MANAGEMENT | AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
Automatically remove temporary and emergency accounts within 72 hours.

(3) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
Disable accounts within one (1) week when the accounts have expired, are no longer associated with a user or individual, are in violation of organizational policy, or have been inactive for 90 calendar days.

(4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
Automatically audit account creation, modification, enabling, disabling, and removal actions.

(5) ACCOUNT MANAGEMENT | INACTIVITY LOGOUT

10/01/2024 - The control is not sanctionable for audit until October 1, 2024.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
Require that users log out when a work period has been completed.
This is a control that should also be part of any agency remote work policy.

(13) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
Disable accounts of individuals within 30 minutes of discovery of direct threats to the confidentiality, integrity, or availability of CJI.
Close coordination among system administrators, legal staff, human resource managers, and authorizing officials is essential when disabling system accounts for high-risk individuals.

AC-3 ACCESS ENFORCEMENT

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

(14) ACCESS ENFORCEMENT | INDIVIDUAL ACCESS

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
Provide automated or manual processes to enable individuals to have access to elements of their personally identifiable information.
Individual access affords individuals the ability to review personally identifiable information about them held within organizational records, regardless of format. Access helps individuals to develop an understanding about how their personally identifiable information is being processed. It can also help individuals ensure that their data is accurate.
Organizational personnel consult with the senior agency official for privacy and legal counsel to determine appropriate mechanisms and access rights or limitations.

AC-4 INFORMATION FLOW ENFORCEMENT

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
The agency is required to enforce approved authorizations for controlling the flow of information within the system and between connected systems by preventing CJI from being transmitted unencrypted across the public network, blocking outside traffic that claims to be from within the agency, and not passing any web requests to the public network that are not from the agency-controlled or internal boundary protection devices (e.g., proxies, gateways, firewalls, or routers).

AC-5 SEPARATION OF DUTIES

Current - The control is currently sanctionable for audit.

NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to identify and document separation of duties based on specific duties, operations, or information systems, as necessary, to mitigate risk to CJI and define system access authorizations to support separation of duties.

Separation of duties is enforced through the account management activities in AC-2, access control mechanisms in AC-3, and identity management activities in IA-2, IA-4, and IA-12.

AC-6 LEAST PRIVILEGE

Current - The control is currently sanctionable for audit.

NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions.

(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

Current - The control is currently sanctionable for audit.

NOTE: The agency will need skilled IT resources to be able to meet this requirement.

Authorize access for personnel including security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information security personnel, maintainers, system programmers, etc.) to established system accounts, configured access authorizations (i.e., permissions, privileges), set events to be audited, set intrusion detection parameters, and other security functions and security-relevant information in hardware, software, and firmware.

Security-relevant information includes filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists.

(2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

Current - The control is currently sanctionable for audit.

NOTE: The agency will need skilled IT resources to be able to meet this requirement.

Require that users of system accounts (or roles) with access to privileged security functions or security-relevant information (e.g., audit logs), use non-privileged accounts or roles, when accessing non-security functions.

DPS will be focusing on this control as part of the Technical Audit, requesting a user account list that demonstrates end-users with privileged accounts also have non-privileged accounts, if the end-user has a need for a non-privileged account.

(5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS

Current - The control is currently sanctionable for audit.

NOTE: The agency will need skilled IT resources to be able to meet this requirement.

Restrict privileged accounts on the system to privileged users.

Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Organizations may differentiate in the application of restricting privileged accounts between allowed privileges for local accounts and for domain accounts, provided that they retain the ability to control system configurations for key parameters and as otherwise necessary to sufficiently mitigate risk.

(7) LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES

Current - The control is currently sanctionable for audit.

NOTE: The agency will need skilled IT resources to be able to meet this requirement.

Review annually the privileges assigned to non-privileged and privileged users to validate the need for such privileges and reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

(9) LEAST PRIVILEGE | LOG USE OF PRIVILEGED FUNCTIONS

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
Log the execution of privileged functions.
The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations.

(10) LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
Prevent non-privileged users from executing privileged functions.

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

Mixed - This control is a mixture of currently sanctionable controls and controls not sanctionable until October 1, 2024
The agency is required to enforce a limit of five (5) consecutive invalid logon attempts by a user during a 15-minute time period and automatically lock the account or node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

AC-8 SYSTEM USE NOTIFICATION

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
The agency is required to display a system use notification message to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
Users are accessing a restricted information system.
System usage may be monitored, recorded, and subject to audit.
Unauthorized use of the system is prohibited and subject to criminal and civil penalties.
Use of the system indicates consent to monitoring and recording.
Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.
For publicly accessible systems:
Display system use information consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines, before granting further access to the publicly accessible system.
Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.
Include a description of the authorized uses of the system.
This requirement is nothing new, nor is the requirement to acknowledge the usage conditions to access the system. Regardless, this is something the agency will need to ensure web-based solutions are presenting this message before the end-user gains access to the system. Keep in mind, the end-user must acknowledge this message before they electronically access CJI, at least once, which may be at the agency Windows domain during login.

AC-11 DEVICE LOCK

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to prevent further access to the system by initiating a device lock after a maximum of thirty (30) minutes of inactivity and requiring the user to initiate a device lock before leaving the system

unattended and retain the device lock until the user reestablishes access using established identification and authentication procedures.

EXCEPTION: In the interest of safety, devices that are part of a criminal justice conveyance (i.e., marked/unmarked unit, mobile command station ; NOT a horse, motorcycle, bicycle, or Segway) or used to perform dispatch functions and located within a physically secure location or terminals designated solely for the purpose of receiving alert notifications (i.e., receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement.

(1) DEVICE LOCK | PATTERN-HIDING DISPLAYS

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Conceal, via the device lock, information previously visible on the display with a publicly viewable image. The pattern-hiding display can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

AC-12 SESSION TERMINATION

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

Automatically terminate a user session after a user has been logged out.

Session termination ends all processes associated with a user's logical session except for those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated.

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to identify any specific user actions that can be performed on the system without identification or authentication consistent with organizational mission and business functions. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

AC-17 REMOTE ACCESS

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed and authorize each type of remote access to the system prior to allowing such connections.

The DPS Technical Audit team will be requesting documented step-by-step procedures for ALL methods of remote access in use, or to be used, to access the agency secure network, or systems used to process CJI. This includes agency remote workers, IT Support, vendors, etc. basically, if anyone is outside an agency secure location and is connecting to the agency secure network, they are utilizing remote access. In addition to the step-by-step documentation, the method of encryption in use, which includes a NIST certificate validating the encryption meets the NIST 140-2/3 requirement which can be obtained at the following link: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search

Currently, remote access requires Advanced Authentication (AA), which can still be found in CJISSECPOL IA-5 AUTHENTICATOR MANAGEMENT and IA-5 (1)(a) MEMORIZED SECRETS. On October 1, 2024, Multi-Factor Authentication (MFA) will be required for all remote access.

(1) REMOTE ACCESS | MONITORING AND CONTROL

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

Employ automated mechanisms to monitor and control remote access methods.

(2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol that provides end-to-end communications security over networks and is used for Internet communications and online transactions.

If CJI is accessed during a remote access system, the encryption must be NIST certified FIPS 140-2/3.

(3) REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Route remote accesses through authorized and managed network access control points.

(4) REMOTE ACCESS | PRIVILEGED COMMANDS AND ACCESS

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for compelling operational needs and document the rationale for remote access in the security plan for the system.

Remote access to systems represents a significant potential vulnerability that can be exploited by adversaries. As such, restricting the execution of privileged commands and access to security-relevant information via remote access reduces the exposure of the organization and the susceptibility to threats by adversaries to the remote access capability.

AC-18 WIRELESS ACCESS

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access and authorize each type of wireless access to the system prior to allowing such connections.

(1) WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to protect wireless access to the system using authentication of authorized users and agency-controlled devices, and encryption.

To protect systems with wireless access points, strong authentication of users and devices along with strong encryption can reduce susceptibility to threats by adversaries involving wireless technologies.

(3) WIRELESS ACCESS | DISABLE WIRELESS NETWORKING

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

In addition, the agency/end-user should be aware of the potential security vulnerabilities in regard to leaving wireless technology enabled on an agency issued mobile device when it is not needed.

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Current - The control is currently sanctionable for audit.

NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas and authorize the connection of mobile devices to organizational systems.

Mobile devices are typically associated with a single individual. Protection and control of mobile devices is behavior or policy-based and requires users to take physical action to protect and control such devices when outside of controlled areas.

(5) ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE OR CONTAINER-BASED ENCRYPTION

Current - The control is currently sanctionable for audit.

NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to employ full-device encryption to protect the confidentiality and integrity of information on full- and limited-feature operating system mobile devices authorized to process, store, or transmit CJI.

Container-based encryption provides a more fine-grained approach to data and information encryption on mobile devices, including encrypting selected data structures such as files, records, or fields.

AC-20 USE OF EXTERNAL SYSTEMS

Current - The control is currently sanctionable for audit.

NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to establish agency-level policies governing the use of external systems consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

1. Access the system from external systems; and
2. Process, store, or transmit organization-controlled information using external systems; or

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

Prohibit the use of personally owned information systems including mobile devices (i.e., bring your own device [BYOD]) and publicly accessible systems for accessing, processing, storing, or transmitting CJI.

Consider this with vendors accessing your secure network. How does the agency validate the vendor systems are meeting your agency requirements. Regarding agency employees, good luck trying to get them to agree to install Mobile Device Management (MDM) on an employee's personal mobile device. MDM is usually the end of any agency proposed BYOD policy.

CAUTION: Personal devices connecting to agency secure networks may open the owner of the personal device up to being issued a subpoena for their personal device, and everything on it.

The agency will want to read the Discussion section on this security control in the CJISSECPOL.

(1) USE OF EXTERNAL SYSTEMS | LIMITS ON AUTHORIZED USE

Current - The control is currently sanctionable for audit.

NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans or retention of approved system connection or processing agreements with the organizational entity hosting the external system.

Limiting authorized use recognizes circumstances where individuals using external systems may need to access organizational systems. Organizations need assurance that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been implemented can be achieved by external, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

(2) USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES — RESTRICTED USE

Current - The control is currently sanctionable for audit.

NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.

Please refer to section 5.8 MEDIA PROTECTION (MP)

AC-21 INFORMATION SHARING

Current - The control is currently sanctionable for audit.

NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for as defined in an executed information exchange agreement and employ attribute-based access control (see AC-2(d)(3)) or manual processes as defined in information exchange agreements to assist users in making information sharing and collaboration decisions.

AC-22 PUBLICLY ACCESSIBLE CONTENT

Current - The control is currently sanctionable for audit.

NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to designate individuals authorized to make information publicly accessible, train authorized individuals to ensure that publicly accessible information does not contain nonpublic information, review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included and review the content on the publicly accessible system for nonpublic information quarterly and remove such information, if discovered.

5.16 MAINTENANCE

MA-1 POLICY AND PROCEDURES

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

NOTE: The agency may need skilled IT resources to be able to meet this requirement.

This is where the agency establishes and documents agency policy, including Purpose, Scope, Roles, Responsibilities, Management Commitment, Coordination among agency entities, Compliance and step by step procedures as to how the policy will be implemented at the agency.

The agency must designate an individual with security responsibilities to manage the development, documentation, and dissemination of the agency policies and procedures, and review and update the policy annually, and after any security incidents.

MA-2 CONTROLLED MAINTENANCE

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location. Require that organizational personnel with information security and privacy responsibilities explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement. Sanitize equipment to remove information from associated media prior to removal from organizational facilities for off-site maintenance, repair, replacement, or destruction. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions and include the following information in organizational maintenance records:

1. Component name
2. Component serial number
3. Date/time of maintenance
4. Maintenance performed
5. Name(s) of entity performing maintenance including escort if required.

MA-3 MAINTENANCE TOOLS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to approve, control, and monitor the use of system maintenance tools and review previously approved system maintenance tools prior to each use.

Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website. Such tools can be vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into systems. Maintenance tools can include hardware and software diagnostic test equipment and packet sniffers.

(1) MAINTENANCE TOOLS | INSPECT TOOLS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

Maintenance tools can be directly brought into a facility by maintenance personnel or downloaded from a vendor's website. If, upon inspection of the maintenance tools, organizations determine that the tools have been modified in an improper manner or the tools contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.

(2) MAINTENANCE TOOLS | INSPECT MEDIA

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Check media containing diagnostic and test programs for malicious code before the media are used in the system.

If, upon inspection of media containing maintenance, diagnostic, and test programs, organizations determine that the media contains malicious code, the incident is handled consistent with organizational incident handling policies and procedures.

(3) MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Prevent the removal of maintenance equipment containing organizational information by:
Verifying that there is no organizational information contained on the equipment.
Sanitizing or destroying the equipment.
Retaining the equipment within the facility or
Obtaining an exemption from organizational personnel with system maintenance responsibilities explicitly authorizing removal of the equipment from the facility.

MA-4 NONLOCAL MAINTENANCE

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to approve and monitor nonlocal maintenance and diagnostic activities.

Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system.

Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.

Maintain records for nonlocal maintenance and diagnostic activities and terminate session and network connections when nonlocal maintenance is completed.

The agency should consider non-local maintenance to be remote access for privileged access and ensure the relevant controls are capable of being met, the procedures are documented, and approved by organizational

personnel with security responsibilities, prior to the remote access being formally established, and monitoring the session remote access session when the remote access session is formally established.
Do not let IT Support working outside an agency secure location access to the agency secure network by using Microsoft Remote Desktop unless the requirements for remote access have been met. IT Support may be special, but they have zero exemptions in the CJISSECPOL requirements, and especially not regarding remote access.

MA-5 MAINTENANCE PERSONNEL

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
The agency is required to establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.
Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations and
Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
Please ensure the maintenance personnel have been through Personnel Screening, completed the appropriate Awareness Training, and appropriate Management Control Agreement or CJIS Security Addendum has been fully executed.

MA-6 TIMELY MAINTENANCE

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
The agency is required to obtain maintenance support and/or spare parts for critical system components that process, store, and transmit CJI within agency-defined recovery time and recovery point objectives of failure.
Be Prepared!

CJISSECPOL v5.9.4

The FBI officially released CJISSECPOL version 5.9.4 December 20, 2023. Yet, I remember getting it on February 28, 2024. This is the version the DPS Technical Audit team has locked in for the current audit cycle, which includes all the currently sanctionable controls. The next DPS CJIS Technical Audit cycle will be based upon the CJISSECPOL that is released at that time.

This release was limited to the Audit and Accountability, Physical and Environmental Protection, Systems and Communications Protection, Planning, Contingency Planning, and Risk Assessment security controls. Specifically,

5.4 AUDIT AND ACCOUNTABILITY (AU)

- AU-1 POLICY AND PROCEDURES
- AU-2 EVENT LOGGING
- AU-3 CONTENT OF AUDIT RECORDS
  - (1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION
  - (3) CONTENT OF AUDIT RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS
- AU-4 AUDIT LOG STORAGE CAPACITY
- AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES
- AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING
  - (1) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | AUTOMATED PROCESS INTEGRATION
  - (3) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT RECORD REPOSITORIES
- AU-7 AUDIT RECORD REDUCTION AND REPORT GENERATION
  - (1) AUDIT RECORD REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING
- AU-8 TIME STAMPS
- AU-9 PROTECTION OF AUDIT INFORMATION
  - (1) PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS
- AU-11 AUDIT RECORD RETENTION
- AU-12 AUDIT RECORD GENERATION

5.9 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

- PE-1 POLICY AND PROCEDURES
- PE-2 PHYSICAL ACCESS AUTHORIZATIONS
- PE-3 PHYSICAL ACCESS CONTROL
- PE-4 ACCESS CONTROL FOR TRANSMISSION
- PE-5 ACCESS CONTROL FOR OUTPUT DEVICES
- PE-6 MONITORING PHYSICAL ACCESS
  - (1) MONITORING PHYSICAL ACCESS | INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT
- PE-8 VISITOR ACCESS RECORDS

5.4 AUDIT AND ACCOUNTABILITY (AU)

AU-1 POLICY AND PROCEDURES

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

This is where the agency establishes and documents agency policy, including Purpose, Scope, Roles, Responsibilities, Management Commitment, Coordination among agency entities, Compliance and step by step procedures as to how the policy will be implemented at the agency.

The agency must designate an individual with security responsibilities to manage the development, documentation, and dissemination of the agency policies and procedures, and review and update the policy annually, and after any security incidents.

AU-2 EVENT LOGGING

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to identify the types of events that the system is capable of logging in support of the audit function: authentication, file use, user/group management, events sufficient to establish what occurred, the sources of events, outcomes of events, and operational transactions (e.g., NCIC, III).
Coordinate the event logging function with other organizational entities requiring audit- related information to guide and inform the selection criteria for events to be logged.
Specify the following event types for logging within the system:

All successful and unsuccessful:
System log-on attempts

Attempts to use:
- Access permission on a user account, file, directory, or other system resource.
- Create permission on a user account, file, directory, or other system resource.
- Write permission on a user account, file, directory, or other system resource.
- Delete permission on a user account, file, directory, or other system resource.
- Change permission on a user account, file, directory, or other system resource.

Attempts to change account passwords.
Actions by privileged accounts (i.e., root, Oracle, DBA, admin, etc.).
Attempts for users to: a. Access the audit log file.
Modify the audit log file.
Destroy the audit log file.
Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents and
Review and update the event types selected for logging annually.

AU-3 CONTENT OF AUDIT RECORDS

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to ensure that audit records contain information that establishes the following:
- What type of event occurred.
- When the event occurred.
- Where the event occurred.
- Source of the event.
- Outcome of the event and
- Identity of any individuals, subjects, or objects/entities associated with the event.

(1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Generate audit records containing the following additional information:
- Session, connection, transaction, and activity duration.
- Source and destination addresses.
- Object or filename involved and
- Number of bytes received, and bytes sent (for client-server transactions) in the audit records for audit events identified by type, location, or subject.
- The III portion of the log shall clearly identify:
  - The operator.
  - The authorized receiving agency.
  - The requestor.
  - The secondary recipient.

(3) CONTENT OF AUDIT RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: minimum PII necessary to achieve the purpose for which it is collected.

AU-4 AUDIT LOG STORAGE CAPACITY

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Allocate audit log storage capacity to accommodate the collection of audit logs to meet retention requirements listed in AU-11.
Regardless of the sanctionable date, if the agency has an agency-owned Live Scan devices, please ensure the log files do not fill up and crash the system. This could occur and seriously impact the agency booking process.

AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to alert organizational personnel with audit and accountability responsibilities and system/network administrators within one (1) hour in the event of an audit logging process failure and
Restart all audit logging processes and verify system(s) are logging properly.

AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to review and analyze system audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity.
Report findings to organizational personnel with audit review, analysis, and reporting responsibilities and organizational personnel with information security and privacy responsibilities and
Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

(1) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | AUTOMATED PROCESS INTEGRATION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

Integrate audit record review, analysis, and reporting processes using automated mechanisms.

(3) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT RECORD REPOSITORIES

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

AU-7 AUDIT RECORD REDUCTION AND REPORT GENERATION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to provide and implement an audit record reduction and report generation capability that supports on-demand audit record review, analysis, and reporting requirements and after- the-fact investigations of incidents and does not alter the original content or time ordering of audit records.
Please test the agency ability to meet this requirement by requesting a report on a secure system testing the agency audit reporting capabilities.
For example: Who has logged in, or attempted to log in, to the agency Live Scan device in the past thirty (30) days?
If you find yourself, or the agency staff, is parsing through Windows Event Logs, you will soon realize you need a better method to obtain this type of reporting information. There are numerous Security Information and Event Monitoring (SIEM) tools available on the market. The agency is going to need such tools to meet many of the CJIS requirements. This is one of those controls where a SIEM tool is needed.

(1) AUDIT RECORD REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: information included in AU-3.

AU-8 TIME STAMPS

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to use internal system clocks to generate time stamps for audit records.
Record time stamps for audit records that meet hundredths of a second (i.e., hh:mm:ss:00) interval and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

AU-9 PROTECTION OF AUDIT INFORMATION

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to protect audit information and audit logging tools from unauthorized access, modification, and deletion and
Alert organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators upon detection of unauthorized access, modification, or deletion of audit information.

(1) PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
Authorize access to management of audit logging functionality to only organizational personnel with audit and accountability responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators.

AU-11 AUDIT RECORD RETENTION

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to retain audit records for a minimum of one (1) year or until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

AU-12 AUDIT RECORD GENERATION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on all systems generating required audit logs.
Allow organizational personnel with audit record generation responsibilities, organizational personnel with information security and privacy responsibilities, and system/network administrators to select the event types that are to be logged by specific components of the system and
Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

5.9 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

PE-1 POLICY AND PROCEDURES

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
This is where the agency establishes and documents agency policy, including Purpose, Scope, Roles, Responsibilities, Management Commitment, Coordination among agency entities, Compliance and step by step procedures as to how the policy will be implemented at the agency.

The agency must designate an individual with security responsibilities to manage the development, documentation, and dissemination of the agency policies and procedures, and review and update the policy annually, and after any security incidents.

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides.
Issue authorization credentials for facility access.
Review the access list detailing authorized facility access by individuals annually and when personnel changes occur, and
Remove individuals from the facility access list when access is no longer required.
Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include ID badges, identification cards, and smart cards.

PE-3 PHYSICAL ACCESS CONTROL

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to enforce physical access authorizations by:
Verifying individual access authorizations before granting access to the facility, and
Controlling ingress and egress to the facility using agency-implemented procedures and controls.
Maintain physical access audit logs for the physically secure location and agency-defined sensitive areas.
Control access to areas within the facility designated as non-publicly accessible by implementing physical access devices including, but not limited to keys, locks, combinations, biometric readers, placards, and/or card readers.
Escort visitors and control visitor activity in all physically secure locations.
Secure keys, combinations, and other physical access devices.
Inventory all agency-issued physical access devices annually, and
Change combinations and keys when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.
If the above conditions cannot be met refer to the requirements listed in PE-17.
Physical access control applies to employees and visitors. Individuals with permanent physical access authorizations are not considered visitors. Physical access controls for publicly accessible areas may include physical access control logs/records, guards, or physical access devices and barriers to prevent movement from publicly accessible areas to non-public areas.
Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include facility access points, interior access points to systems that require supplemental access controls, or both. Components of systems may be in areas designated as publicly accessible with organizations controlling access to the components.

PE-4 ACCESS CONTROL FOR TRANSMISSION

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to control physical access to information system distribution and transmission lines and devices within organizational facilities using agency-implemented procedures and controls.
Security controls applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Security controls used to control physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, protection of cabling by conduit or cable trays, and wiretapping sensors.

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to control physical access to output from monitors, printers, scanners, audio devices, facsimile machines, and copiers to prevent unauthorized individuals from obtaining the output.

PE-6 MONITORING PHYSICAL ACCESS

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to monitor physical access to the facility where the system resides to detect and respond to physical security incidents.
Review physical access logs quarterly and upon occurrence of any physical, environmental, or security-related incidents involving CJI, or systems used to process, store, or transmit CJI, and
Coordinate results of reviews and investigations with the organizational incident response capability.

(1) MONITORING PHYSICAL ACCESS | INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.
Maintain visitor access records to the facility where the system resides for one (1) year.
Review visitor access records quarterly, and
Report anomalies in visitor access records to organizational personnel with physical and environmental protection responsibilities and organizational personnel with information security responsibilities.

PE-8 VISITOR ACCESS RECORDS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to maintain visitor access records to the facility where the system resides for one (1) year.
Review visitor access records quarterly, and
Report anomalies in visitor access records to organizational personnel with physical and environmental protection responsibilities and organizational personnel with information security responsibilities.
Visitor access records include the names and organizations of individuals visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purpose of visits, and the names and organizations of individuals visited. Access record reviews determine if access authorizations are current and are still required to support organizational mission and business functions. Access records are not required for publicly accessible areas.

(3) VISITOR ACCESS RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to limit personally identifiable information contained in visitor access records to the minimum PII necessary to achieve the purpose for which it is collected.
Note: Access to visitor access records is restricted to authorized agency personnel.

PE-9 POWER EQUIPMENT AND CABLING

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to protect power equipment and power cabling for the system from damage and destruction.
NOTE: This control only applies to data centers which is defined as: A physical room, building, or facility housing Information Technology infrastructure for developing, running, and delivering applications and services associated with storing and managing data, as determined by the CSO, his/her designee, or Interface Agency Official.

PE-10 EMERGENCY SHUTOFF

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to provide the capability of shutting off power to all information systems in emergency situations.
Place emergency shutoff switches or devices in easily accessible locations to facilitate access for authorized personnel, and
Protect emergency power shutoff capability from unauthorized activation.

Emergency power shutoff primarily applies to organizational facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, server rooms, and areas with computer-controlled machinery.
NOTE: This control only applies to data centers which is defined as: A physical room, building, or facility housing Information Technology infrastructure for developing, running, and delivering applications and services associated with storing and managing data, as determined by the CSO, his/her designee, or Interface Agency Official.
Emergency power shutoff primarily applies to organizational facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, server rooms, and areas with computer-controlled machinery.

PE-11 EMERGENCY POWER

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to provide an uninterruptible power supply to facilitate an orderly shutdown of the information system or transition of the information system to an alternate power source in the event of a primary power source loss.
NOTE: This control only applies to data centers which is defined as: A physical room, building, or facility housing Information Technology infrastructure for developing, running, and delivering applications and services associated with storing and managing data, as determined by the CSO, his/her designee, or Interface Agency Official.

PE-12 EMERGENCY LIGHTING

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.
NOTE: This control only applies to data centers which is defined as: A physical room, building, or facility housing Information Technology infrastructure for developing, running, and delivering applications and services associated with storing and managing data, as determined by the CSO, his/her designee, or Interface Agency Official.

PE-13 FIRE PROTECTION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to employ and maintain fire detection and suppression systems that are supported by an independent energy source.
NOTE: This control only applies to data centers which is defined as: A physical room, building, or facility housing Information Technology infrastructure for developing, running, and delivering applications and services associated with storing and managing data, as determined by the CSO, his/her designee, or Interface Agency Official.
The provision of fire detection and suppression systems applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Fire detection and suppression systems that may require an independent energy source include sprinkler systems and smoke detectors. An independent energy source is an energy source, such as a microgrid, that is separate, or can be separated, from the energy sources providing power for the other parts of the facility.

(1) FIRE PROTECTION | DETECTION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
Employ fire detection systems that activate automatically and notify organizational personnel with physical and environmental protection responsibilities and police, fire, or emergency medical personnel in the event of a fire.

NOTE: This control only applies to data centers which is defined as: A physical room, building, or facility housing Information Technology infrastructure for developing, running, and delivering applications and services associated with storing and managing data, as determined by the CSO, his/her designee, or Interface Agency Official.
Organizations can identify personnel, roles, and emergency responders if individuals on the notification list need to have access authorizations or clearances (e.g., to enter to facilities where access is restricted due to the classification or impact level of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

PE-14 ENVIRONMENTAL CONTROLS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to maintain adequate HVAC levels within the facility where the system resides at recommended system manufacturer levels, and
Monitor environmental control levels continuously.
NOTE: This control only applies to data centers which is defined as: A physical room, building, or facility housing Information Technology infrastructure for developing, running, and delivering applications and services associated with storing and managing data, as determined by the CSO, his/her designee, or Interface Agency Official.
The provision of environmental controls applies primarily to organizational facilities that contain concentrations of system resources (e.g., data centers, mainframe computer rooms, and server rooms). Insufficient environmental controls, especially in very harsh environments, can have a significant adverse impact on the availability of systems and system components that are needed to support organizational mission and business functions.

PE-15 WATER DAMAGE PROTECTION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.
NOTE: This control only applies to data centers which is defined as: A physical room, building, or facility housing Information Technology infrastructure for developing, running, and delivering applications and services associated with storing and managing data, as determined by the CSO, his/her designee, or Interface Agency Official.
The provision of water damage protection primarily applies to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern without affecting entire organizations.

PE-16 DELIVERY AND REMOVAL

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to authorize and control information system-related components entering and exiting the facility, and
Maintain records of the system components.
Enforcing authorizations for entry and exit of system components may require restricting access to delivery areas and isolating the areas from the system and media libraries.

PE-17 ALTERNATE WORK SITE

Current - The control is currently sanctionable for audit.
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to determine and document all alternate facilities or locations allowed for use by employees.
Employ the following controls at alternate work sites:

Limit access to the area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
Lock the area, room, or storage container when unattended.
Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
Follow the encryption requirements found in SC-13 and SC-28 for electronic storage (i.e., data at-rest) of CJI.

Assess the effectiveness of controls at alternate work sites; and
Provide a means for employees to communicate with information security and privacy personnel in case of incidents.
Alternate work sites include government facilities or the private residences of employees. While distinct from alternative processing sites, alternate work sites can provide readily available alternate locations during contingency operations. Organizations can define different sets of controls for specific alternate work sites or types of sites depending on the work-related activities conducted at the sites. Implementing and assessing the effectiveness of organization-defined controls and providing a means to communicate incidents at alternate work sites supports the contingency planning activities of organizations.

5.10 SYSTEMS AND COMMUNICATIONS PROTECTION (SC)

SC-1 POLICY AND PROCEDURES

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
This is where the agency establishes and documents agency policy, including Purpose, Scope, Roles, Responsibilities, Management Commitment, Coordination among agency entities, Compliance and step by step procedures as to how the policy will be implemented at the agency.

The agency must designate an individual with security responsibilities to manage the development, documentation, and dissemination of the agency policies and procedures, and review and update the policy annually, and after any security incidents.

SC-2 SEPARATION OF SYSTEM AND USER FUNCTIONALITY

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
The agency is required to separate user functionality, including user interface services, from system management functionality.

SC-4 INFORMATION IN SHARED SYSTEM RESOURCES

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
The agency is required to prevent unauthorized and unintended information transfer via shared system resources.

SC-5 DENIAL-OF-SERVICE PROTECTION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
The agency is required to protect against or limit the effects of denial-of-service events, distributed denial of service, DNS Denial of Service, etc., and employ the following controls to achieve the denial-of-service objective: boundary protection devices and intrusion detection or prevention devices.

SC-7 BOUNDARY PROTECTION

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system.
Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks, and
Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

(3) BOUNDARY PROTECTION | ACCESS POINTS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
Limit the number of external network connections to the system.

(4) BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
Implement a managed interface for each external telecommunication service.
Establish a traffic flow policy for each managed interface.
Protect the confidentiality and integrity of the information being transmitted across each interface.
Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need.
Review exceptions to the traffic flow policy annually, after any incident, and after any major changes impacting the information system, while removing exceptions that are no longer supported by an explicit mission or business need.
Prevent unauthorized exchange of control plane traffic with external networks.
Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks, and
Filter unauthorized control plane traffic from external networks.

(5) BOUNDARY PROTECTION | DENY BY DEFAULT — ALLOW BY EXCEPTION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
Deny network communications traffic by default and allow network communications traffic by exception at boundary devices for information systems used to process, store, or transmit CJI.

(7) BOUNDARY PROTECTION | SPLIT TUNNELING FOR REMOTE DEVICES

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
Prevent split tunneling for remote devices connecting to organizational systems.

(8) BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
Route all internal communications traffic that may be proxied, except traffic specifically exempted by organizational personnel with information security responsibilities, to all untrusted networks through authenticated proxy servers at managed interfaces.

(24) BOUNDARY PROTECTION | PERSONALLY IDENTIFIABLE INFORMATION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
For systems that process personally identifiable information:

Apply the following processing rules to data elements of personally identifiable information: all applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system.
Document each processing exception, and
Review and remove exceptions that are no longer supported.

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to protect the confidentiality and integrity of transmitted information. Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.

(1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

Implement cryptographic mechanisms to prevent unauthorized disclosure and detect unauthorized changes or access to CJI during transmission.

SC-10 NETWORK DISCONNECT

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to terminate the network connection associated with a communications session at the end of the session or after one (1) hour of inactivity.
NOTE: In the interest of safety, devices that are: part of a criminal justice conveyance; or used to perform dispatch functions and located within a physically secure location; or terminals designated solely for the purpose of receiving alert notifications (i.e., receive only terminals or ROT) and used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: encryption key generation, distribution, storage, access, and destruction is controlled by the agency.
Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations manage trust stores to ensure that only approved trust anchors are part of such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems.

SC-13 CRYPTOGRAPHIC PROTECTION

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to determine the use of encryption for CJI in-transit when outside a physically secure location and
Implement the following types of cryptography required for each specified cryptographic use: cryptographic modules which are Federal Information Processing Standard (FIPS) 140-3 certified, or FIPS validated algorithm for symmetric key encryption and decryption (FIPS 197 [AES]), with a symmetric cipher key of at least 128-bit strength for CJI in-transit.
NOTE: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-3 compliancy can be used in the interim until certification is complete. FIPS 140-2 certificates will not be acceptable after September 21, 2026.

SC-15 COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to prohibit remote activation of collaborative computing devices and applications and provide an explicit indication of use to users physically present at the devices.

Collaborative computing devices and applications include remote meeting devices and applications, networked white boards, cameras, and microphones. The explicit indication of use includes signals to users when collaborative computing devices and applications are activated.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to issue public key certificates under an agency-level certificate authority or obtain public key certificates from an approved service provider and include only approved trust anchors in trust stores or certificate stores managed by the organization.

Public key infrastructure (PKI) certificates are certificates with visibility external to organizational systems and certificates related to the internal operations of systems, such as application-specific time services. In cryptographic systems with a hierarchical structure, a trust anchor is an authoritative source (i.e., a certificate authority) for which trust is assumed and not derived. A root certificate for a PKI system is an example of a trust anchor. A trust store or certificate store maintains a list of trusted root certificates.

SC-18 MOBILE CODE

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to define acceptable and unacceptable mobile code and mobile code technologies and authorize, monitor, and control the use of mobile code within the system.

Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. Decisions regarding the use of mobile code within organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include Java applets, JavaScript, HTML5, WebGL, and VBScript. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices, including notebook computers and smart phones.

SC-20 SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries and provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

SC-21 SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Systems that provide name and address resolution services for local clients include recursive resolving or caching domain name system (DNS) servers.

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

SC-23 SESSION AUTHENTICITY

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

NOTE: The agency will need skilled IT resources to be able to meet this requirement.
The agency is required to protect the authenticity of communications sessions.

SC-28 PROTECTION OF INFORMATION AT REST

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
The agency is required to protect the confidentiality and integrity of the following information at rest: CJI when outside physically secure locations using cryptographic modules which are certified FIPS 140-3 with a symmetric cipher key of at least 128-bit strength, or FIPS 197 with a symmetric cipher key of at least 256-bit strength.
Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.
The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g., government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e., United States, U.S. territories, Indian Tribes, and Canada) and are under legal authority of an APB-member agency (i.e., United States–federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police).
This restriction does not apply to exchanges of CJI with foreign government agencies under international exchange agreements (e.g., the Preventing and Combating Serious Crime agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).
NOTE: The State of Texas has enhanced this requirement in the Texas CJIS Security Policy Supplement:

> ***Third-Party Cloud Services Providers***
> ***For agency proposed hosted services using a third-party Cloud Services Provider (CSP), these agency solutions if used to process, store, or transmit CJI must be deployed in a DPS approved government cloud environment and/or National Law Enforcement Telecommunications System (NLETS).***

(1) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the CJI At Rest on information systems and digital media outside physically secure locations.
Encryption must be FIPS 197 certified (AES 256-bit).

SC-39 PROCESS ISOLATION

Current - The control is currently sanctionable for audit.
NOTE: The agency will need skilled IT resources to be able to meet this requirement.
Maintain a separate execution domain for each executing system process.

5.17 PLANNING (PL)

PL-1 POLICY AND PROCEDURES

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
This is where the agency establishes and documents agency policy, including Purpose, Scope, Roles, Responsibilities, Management Commitment, Coordination among agency entities, Compliance and step by step procedures as to how the policy will be implemented at the agency.

The agency must designate an individual with security responsibilities to manage the development, documentation, and dissemination of the agency policies and procedures, and review and update the policy annually, and after any security incidents.

PL-2 SYSTEM SECURITY AND PRIVACY PLANS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to develop security and privacy plans for the system that: 1. Are consistent with the organization's enterprise architecture.
Explicitly define the constituent system components.
Describe the operational context of the system in terms of mission and business processes.
Identify the individuals that fulfill system roles and responsibilities.
Identify the information types processed, stored, and transmitted by the system.
Provide the security categorization of the system, including supporting rationale.
Describe any specific threats to the system that are of concern to the organization.
Provide the results of a privacy risk assessment for systems processing personally identifiable information.
Describe the operational environment for the system and any dependencies on or connections to other systems or system components.
Provide an overview of the security and privacy requirements for the system.
Identify any relevant control baselines or overlays, if applicable.
Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions.
Include risk determinations for security and privacy architecture and design decisions.
Include security- and privacy-related activities affecting the system that require planning and coordination with organizational personnel with system security and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities, and
Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

Distribute copies of the plans and communicate subsequent changes to the plans to organizational personnel with system security and privacy planning and plan implementation responsibilities, system developers, organizational personnel with information security and privacy responsibilities,
Review the system security and privacy plans at least annually or when required due to system changes or modifications.
Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments, and
Protect the plans from unauthorized disclosure and modification.

PL-4 RULES OF BEHAVIOR

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy.
Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system.
Review and update the rules of behavior at least annually, and
Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge annually, or when the rules are revised or updated.

(1) RULES OF BEHAVIOR | SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Include in the rules of behavior, restrictions on:

Use of social media, social networking sites, and external sites/applications.
Posting organizational information on public websites, and
Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

PL-8 SECURITY AND PRIVACY ARCHITECTURES

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to develop security and privacy architectures for the system that:

Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information.

Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals.

Describe how the architectures are integrated into and support the enterprise architecture; and

Describe any assumptions about, and dependencies on, external systems and services.

Review and update the architectures at least annually or when changes to the system or its environment occur to reflect changes in the enterprise architecture, and

Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

PL-9 CENTRAL MANAGEMENT

10/01/2024 – I am curious as to why this control is not sanctionable for audit until October 1, 2024

The CJISSECPOL is centrally managed by the FBI CJIS ISO.

PL-10 BASELINE SELECTION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to select a control baseline for the system.

Control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Controls are chosen for baselines to either satisfy mandates imposed by laws, executive orders, directives, regulations, policies, standards, and guidelines or address threats common to all users of the baseline under the assumptions specific to the baseline. Baselines represent a starting point for the protection of individuals' privacy, information, and information systems with subsequent tailoring actions to manage risk in accordance with mission, business, or other constraints (see PL-11).

PL-11 BASELINE TAILORING

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to tailor the selected control baseline by applying specified tailoring actions.

The concept of tailoring allows organizations to specialize or customize a set of baseline controls by applying a defined set of tailoring actions. Tailoring actions facilitate such specialization and customization by allowing organizations to develop security and privacy plans that reflect their specific mission and business functions, the environments where their systems operate, the threats and vulnerabilities that can affect their systems, and any other conditions or situations that can impact their mission or business success.

5.18 CONTINGENCY PLANNING (CP)

CP-1 POLICY AND PROCEDURES

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

NOTE: The agency may need skilled IT resources to be able to meet this requirement.

This is where the agency establishes and documents agency policy, including Purpose, Scope, Roles, Responsibilities, Management Commitment, Coordination among agency entities, Compliance and step by step procedures as to how the policy will be implemented at the agency.

The agency must designate an individual with security responsibilities to manage the development, documentation, and dissemination of the agency policies and procedures, and review and update the policy annually, and after any security incidents.

CP-2 CONTINGENCY PLAN

10/01/2024 - The control is not sanctionable for audit until October 1, 2024

NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to develop a contingency plan for the system that: 1. Identifies essential mission and business functions and associated contingency requirements.

Provides recovery objectives, restoration priorities, and metrics.
Addresses contingency roles, responsibilities, assigned individuals with contact information.
Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure.
Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented.
Addresses the sharing of contingency information; and
Is reviewed and approved by agency head or their designee.

Distribute copies of the contingency plan to organizational personnel with contingency planning or incident response duties.
Coordinate contingency planning activities with incident handling activities.
Review the contingency plan for the system annually.
Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.
Communicate contingency plan changes to organizational personnel with contingency planning or incident response duties.
Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training, and
Protect the contingency plan from unauthorized disclosure and modification.
Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached.

(1) CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Coordinate contingency plan development with organizational elements responsible for related plans. Plans that are related to contingency plans include Business Continuity Plans, Disaster Recovery Plans, Critical Infrastructure Plans, Continuity of Operations Plans, Crisis Communications Plans, Insider Threat Implementation Plans, Data Breach Response Plans, Cyber Incident Response Plans, Breach Response Plans, and Occupant Emergency Plans.

(3) CONTINGENCY PLAN | RESUME MISSION AND BUSINESS FUNCTIONS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Plan for the resumption of essential mission and business functions within twenty-four (24) hours of contingency plan activation.

(8) CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Identify critical system assets supporting essential mission and business functions.

CP-3 CONTINGENCY TRAINING

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to provide contingency training to system users consistent with assigned roles and responsibilities:

Within thirty (30) days of assuming a contingency role or responsibility.
When required by system changes. and
Annually thereafter, and

Review and update contingency training content annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI, or training simulations or exercises.

CP-4 CONTINGENCY PLAN TESTING

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to test the contingency plan for the system annually using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), or comprehensive exercises. Review the contingency plan test results and initiate corrective actions, if needed.

(1) CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Coordinate contingency plan testing with organizational elements responsible for related plans.

CP-6 ALTERNATE STORAGE SITE

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information and ensure that the alternate storage site provides controls equivalent to that of the primary site.

(1) ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

(3) ALTERNATE STORAGE SITE | ACCESSIBILITY

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

CP-7 ALTERNATE PROCESSING SITE

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to establish an alternate processing site, including necessary agreements to permit the transfer and resumption of operations for essential mission and business functions within the time period defined in the system contingency plan(s) when the primary processing capabilities are unavailable.
Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption, and
Provide controls at the alternate processing site that are equivalent to those at the primary site.

(1) ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

(2) ALTERNATE PROCESSING SITE | ACCESSIBILITY

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

(3) ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

CP-8 TELECOMMUNICATIONS SERVICES

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to establish alternate telecommunications services, including necessary agreements to permit the resumption of system operations for essential mission and business functions within the time period as defined in the system contingency plan(s) when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

(1) TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives), and Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

(2) TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

CP-9 SYSTEM BACKUP

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to conduct backups of user-level information contained in operational systems for essential business functions as required by the contingency plans.
Conduct backups of system-level information contained in the system as required by the contingency plans.
Conduct backups of system documentation, including security- and privacy-related documentation as required by the contingency plans, and
Protect the confidentiality, integrity, and availability of backup information.

(1) SYSTEM BACKUP | TESTING FOR RELIABILITY AND INTEGRITY

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
Test backup information as required by the contingency plans to verify media reliability and information integrity.

(8) SYSTEM BACKUP | CRYPTOGRAPHIC PROTECTION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of CJI.

CP-10 SYSTEM RECOVERY AND RECONSTITUTION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to provide for the recovery and reconstitution of the system to a known state within the timeframe as required by the contingency plans after a disruption, compromise, or failure.

(2) SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
Implement transaction recovery for systems that are transaction-based.

5.19 RISK ASSESSMENT (RA)

RA-1 POLICY AND PROCEDURES

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
This is where the agency establishes and documents agency policy, including Purpose, Scope, Roles, Responsibilities, Management Commitment, Coordination among agency entities, Compliance and step by step procedures as to how the policy will be implemented at the agency.

The agency must designate an individual with security responsibilities to manage the development, documentation, and dissemination of the agency policies and procedures, and review and update the policy annually, and after any security incidents.

RA-2 SECURITY CATEGORIZATION

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to categorize the system and information it processes, stores, and transmits. Document the security categorization results, including supporting rationale, in the security plan for the system and verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

RA-3 RISK ASSESSMENT

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.
The agency is required to conduct a risk assessment, including:

- Identifying threats to and vulnerabilities in the system.
- Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information, and
- Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information.

Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments.
Document risk assessment results in a risk assessment report.
Review risk assessment results at least quarterly.
Disseminate risk assessment results to organizational personnel with risk assessment responsibilities and organizational personnel with security and privacy responsibilities, and
Update the risk assessment at least quarterly or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.
Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation. Risk assessments also consider risk from external parties, including contractors who operate systems on behalf of the organization, individuals who access organizational systems, service providers, and outsourcing entities.
Organizations can conduct risk assessments at all three levels in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any stage in the system development life cycle.

RA-5 VULNERABILITY MONITORING AND SCANNING

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

The agency is required to monitor and scan for vulnerabilities in the system and hosted applications at least monthly and when new vulnerabilities potentially affecting the system are identified and reported.
Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

Enumerating platforms, software flaws, and improper configurations.
Formatting checklists and test procedures, and
Measuring vulnerability impact.

Analyze vulnerability scan reports and results from vulnerability monitoring.
Remediate legitimate vulnerabilities within the number of days listed:

- Critical–15 days
- High–30 days
- Medium–60 days
- Low–90 days; and

Share information obtained from the vulnerability monitoring process and control assessments with organizational personnel with risk assessment, control assessment, and vulnerability scanning responsibilities to help eliminate similar vulnerabilities in other systems, and
Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

(2) VULNERABILITY MONITORING AND SCANNING | UPDATE VULNERABILITIES TO BE SCANNED

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Update the system vulnerabilities to be scanned within 24 hours prior to running a new scan or when new vulnerabilities are identified and reported.

(5) VULNERABILITY MONITORING AND SCANNING | PRIVILEGED ACCESS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

Implement privileged access authorization to information system components containing or processing CJI for vulnerability scanning activities requiring privileged access.

(11) VULNERABILITY MONITORING AND SCANNING | PUBLIC DISCLOSURE PROGRAM

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency will need skilled IT resources to be able to meet this requirement.

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

RA-7 RISK RESPONSE

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to respond to finding from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

RA-9 CRITICALITY ANALYSIS

10/01/2024 - The control is not sanctionable for audit until October 1, 2024
NOTE: The agency may need skilled IT resources to be able to meet this requirement.

The agency is required to identify critical system components and functions by performing a criticality analysis for information system components containing or processing CJI at the planning, design, development, testing, implementation, and maintenance stages of the system development life cycle.