CJIS Technical Audit 5.9.4

Preview

Report created: Tue Aug 06 2024 10:13:07 GMT-0500 (Central Daylight Time)

Section - Agency Information

1. Is the agency fully aware the scope of the CJIS technical audit includes all systems used to process and/or store Criminal Justice Information (CJI)?

Definition: CJI is the term used to refer to all of the FBI CJIS Division provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to, biometric, identity history, biographic, property, and case/incident history data (i.e., any information obtained from the FBI).

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until the information is: released to the public via authorized dissemination (e.g. within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules.

TLETS Related Data is considered Criminal Justice Information (CJI), Criminal History Record Information (CHRI), and/or Personal Identifiable Information (PII) derived from query results of a State and/or Federal repositories, such as TCIC/NCIC. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.

Per the TCIC Access Policy: The Department considers any TCIC/NCIC record information and CCH/III information as criminal justice data. Information derived from the Driver License system or the Vehicle Registration system via TLETS contains personal and private information that could be protected by federal or state statute but not by the FBI Security policy.

Criminal Justice Information (CJI) (e.g., TLETS Related Data) taken from FBI or DPS systems and copied, transposed, or scanned into local agency information systems (e.g., a Records Management System [RMS]) is still considered CJI and still falls under the scope of the CJISSECPOL (i.e., the audit).

☐ I have read and understand the above statement.

2. Provide contact details for the Organizational Personnel with Security Responsibilities (LASO) below.

NOTE: If LASO is the same as the TAC, please indicate as TAC/LASO.

3.2.3 Terminal Agency Coordinator (TAC)
The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

3.2.9 Organizational Personnel with Security Responsibilities (Local Agency Security Officer (LASO))
Each LASO shall:
1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

3. Please provide your agency's IBR administrator's name, email and phone number.

4. Please select from the drop down below all of the entities responsible for providing the agency's IT Support.

☐ City Government (Non-criminal Justice Agency)
☐ County Government (Non-criminal Justice Agency)
☐ Vendor (3rd Party Private - Non-criminal Justice)
☐ Internal
☐ Unsure

5. Please select from the drop down below if the agency is being hosted, or is hosting services for other agencies.

○ Hosted (Receives CJI from another agency TLETS/NLETS interface)
○ Hosting (Provides CJI from your agency TLETS/NLETS interface to another agency)
○ Not Applicable
○ Unsure

Primary question answer 1 selected

1. Please provide the agency name which hosts or provides your agency access to TLETS.

Primary question answer 2 selected

1. Please provide names, and ORI's (if known) for all agencies being hosted by your agency.

6. Does the agency use wired devices (desktop, laptop, etc.) to access TLETS/NLETS related data?

○ Yes
○ No

Primary question answered Yes

1. Please provide the total number of wired devices, by type, used to access TLETS/NLETS related data.

7. Does the agency use wireless devices (desktop, MDT, laptop, phone, tablet etc.) to access TLETS/NLETS related data?

○ Yes
○ No

Primary question answered Yes

1. Please provide the total number of wireless devices, by type, used to access TLETS/NLETS data.

8. Does the agency have any fingerprinting device (AFIS Livescan, Latent Print, NEC, MBIS workstation etc.)?

○ Yes
○ No

Primary question answered Yes

1. Please provide the total number of fingerprint devices, by type, used to access TLETS/ NLETS related data.

9. Please provide a list of all applications used by the agency that access, provide access to, process, or store Criminal Justice Information.

Section - Policy Area 1 - Information Exchange Agreements

1. 5.1.1 Information Exchange

Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI.
Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.
Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D of the CJIS Security Policy for examples of Information Exchange Agreements. There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. See Section 5.1.3 for secondary dissemination guidance.

☐ I have read and understand the above statement.

2. Does the agency share CJI with other agencies, or any other entities?

○ Yes
○ No

Primary question answered Yes

1. Please indicate what software solution(s) are used to share CJI.
Please provide your auditor copies of all Interagency Agreements between the agency and any other entities in which CJI is being shared.

5.1.3) If the agency is involved in secondary dissemination of CHRI to an agency that is not party to an existing agreement, please provide the auditor a snippet from the secondary dissemination log of the releasing agency.

Primary question answered No

1. Does any of your vendors share CJI with other agencies or entities?

3. 5.1.1.4 Interagency and Management Control Agreements

Does the agency have a Management Control Agreement for all non-law enforcement governmental support?

5.1.1.4 Interagency and Management Control Agreements
A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or interagency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an interagency agreement. An example of an NCJA (government) is a city information technology (IT) department.

- ○ YES
- ○ NO
- ○ NA

Primary question answer 1 selected

1. Please provide the auditor a copy of all agency Management Control Agreements.

NOTE: The purpose of the MCA is to ensure the agency always maintains management control of all systems used to process, store, and/or transmit CJI.

Primary question answer 2 selected

1. An MCA is required for agencies which are supported through City or County services (non-law enforcement support for IT, Consolidated Dispatch, Forensic services, etc.) when unescorted access or remote access is made available to areas involving CJI.

Please describe below how support is provided for the agency. (example; escort only, etc.)

4. 5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum

Does the agency have individual Security Addendum for all Vendors involved in CJIS systems support or unescorted access to agency secure locations?

The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.
Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H of the CJISSECPOL. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.

1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

○ YES
○ NO
○ NA

Primary question answer 1 selected

1. Please provide a copy of each fully executed Security Addendum to the auditor and ensure they are maintained and kept current with vendor personnel changes.

NOTE: This is a legal document which binds the vendor/subcontractors to the requirements of the CJIS Security Policy.

The Texas version of the Security Addendum is an eight(8)page document, at a minimum.
Page 1: Contact Information
Page 2-6: Legal terms that can ONLY be modified by the FBI.
Page 7: FBI Certification Page - There should be a separate page for all vendor/subcontractor personnel with access to unencrypted CJI, unescorted access to agency secure locations, or administrative access to systems used to process CJI.
Page 8: Texas Signatory Page - The vendor can also have subcontractors sign this page as well.

2. Please provide contact details for the Agency Coordinator(s):

3.2.7 Agency Coordinator (AC)
An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training, and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. The AC shall:
1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
2. Participate in related meetings and provide input and comments for system improvement.
3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.

7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
10. Any other responsibility for the AC promulgated by the CGA.

Primary question answer 2 selected

1. A Security Addendum is required for agencies which are supported through third party vendors or contractors for services (non-law enforcement support for IT services, etc.) when unescorted access or remote access is made available to CJI.

Please describe how support is provided for the agency. (example; escort only, etc.)

Section - Policy Area 2 - Awareness and Training (AT)

1. Does the agency meet the following awareness and training requirements?

AT-1 POLICY AND PROCEDURES
a. Develop, document, and disseminate to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI:
1. Organization-level awareness and training policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;
b. Designate organizational personnel with information security awareness and training responsibilities to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and
c. Review and update the current awareness and training:
1. Policy annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJIS Security Policy are made; and
2. Procedures annually and following changes in the information system operating environment, when security incidents occur, or when changes to the CJIS Security Policy are made.

○ Yes
○ No

Primary question answered Yes

1. Please provide the auditor a copy of the agency's documented Awareness & Training Policy and a copy of the agency's step-by-step procedures.

☐ I have read and will comply.

2. How does the agency validate authorized individuals acknowledge the policy/procedures?

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented, please provide the auditor a copy of the agency's documented Awareness & Training Policy and a copy of the agency's step-by-step procedures.

☐ I have read and will comply.

2. AT-2 LITERACY TRAINING AND AWARENESS

Does the agency:

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):
1. As part of initial training for new users prior to accessing CJI and annually thereafter; and
2. When required by system changes or within 30 days of any security event for individuals involved in the event?
b. Does the agency employ one or more of the following techniques to increase the security and privacy awareness of system users?
1. Displaying posters
2. Offering supplies inscribed with security and privacy reminders
3. Displaying logon screen messages
4. Generating email advisories or notices from organizational officials
5. Conducting awareness events
c. Update literacy training and awareness content annually and following changes in the information system operating environment, when security incidents occur, or when changes are made in the CJIS Security Policy; and
d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques?

(2) LITERACY TRAINING AND AWARENESS | INSIDER THREAT
Does the agency provide literacy training on recognizing and reporting potential indicators of insider threat?

(3) LITERACY TRAINING AND AWARENESS | SOCIAL ENGINEERING AND MINING
Does the agency provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining?

○ Yes
○ No

Primary question answered Yes

1. Please provide the auditor a copy of any agency specific Awareness and Training material.

☐ I have read and will comply.

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented, please provide the auditor a copy of any agency specific Awareness and Training material.

☐ I have read and will comply.

3. AT-3 ROLE-BASED TRAINING & AT-4 TRAINING RECORDS

Have all personnel (Dispatchers, Law Enforcement, IT, Contractors) received appropriate role-based awareness training?

All individuals with unescorted access to a physically secure location;

General User: A user who is authorized to use an information system;

Privileged User: A user that is authorized to perform security-relevant functions that general users are not authorized to perform; (i.e., TAC/SAGY)

Organizational Personnel with Security Responsibilities: 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. (i.e., LASO)

1. Before authorizing access to the system, information, or performing assigned duties, and annually thereafter; and
2. When required by system changes.
b. Does the agency update role-based training content annually and following audits of the CSA and local agencies; changes in the information system operating environment; security incidents; or when changes are made to the CJIS Security Policy;
c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training; and
d. Incorporate the CJIS Security Policy's required topics into the appropriate role-based training content?

5) ROLE-BASED TRAINING | PROCESSING PERSONALLY IDENTIFIABLE INFORMATION
Does the agency provide all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI with initial and annual training in the employment and operation of personally identifiable information processing and transparency controls?

○ Yes
○ No

Primary question answered Yes

1. Please describe the methods used, (ie; CJIS Online, etc.)

If using CJIS Online please provide the auditor a copy of of the Security and Privacy Status Report for all authorized personnel and all authorized vendor personnel.

If not using CJIS Online please provide the auditor verification that your training meets the CJIS Security Policy requirements and provide a report reflecting that all authorized personnel and vendor personnel are current in their training.

---

2. Does the agency retain individual training records for a minimum of three years?

○ Yes
○ No

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented please describe the methods used, (ie; CJIS Online, etc.)

If using CJIS Online please provide the auditor a copy of of the Security and Privacy Status Report for all authorized personnel and all authorized vendor personnel.

If not using CJIS Online please provide the auditor verification that your training meets the CJIS Security Policy requirements and provide a report reflecting that all authorized personnel and vendor personnel are current in their training.

NOTE: Please ensure that individual training records are retained for a minimum of three years.

☐ I have read and will comply.

4. AT-4 TRAINING RECORDS

Does the agency document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and retain individual training records for a minimum of three years?

○ Yes
○ No

Section - Policy Area 3 - Incident Response

1. IR-1 POLICY AND PROCEDURES & IR-8 INCIDENT RESPONSE PLAN

Does the agency:

a. Develop, document, and disseminate to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI:
1. Agency-level incident response policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls?
b. Has the agency designated an individual with security responsibilities to manage the development, documentation, and dissemination of the incident response policy and procedures?

NOTE: Ensure DPS OIC contact information is included, ex: Notify the TLETS Operations Information Center (OIC) at 1-888-DPS-OIC0 (1-888-377-6420) within 1 hour.

○ Yes
○ No

Primary question answered Yes

1. Please provide the auditor a copy of the agency's documented Incident Response Policy and a copy of the agency's step-by-step procedures.

☐ I have read and will comply.

2. How does the agency validate authorized individuals acknowledge the policy/procedures?

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented please provide the auditor a copy of the agency's documented Incident Response Policy and a copy of the agency's step-by-step procedures.

☐ I have read and will comply.

2. IR-2 INCIDENT RESPONSE TRAINING

Does the agency provide incident response training to system users consistent with assigned roles and responsibilities:

1. Prior to assuming an incident response role or responsibility or acquiring system access;
2. When required by system changes; and
3. Annually thereafter?

○ Yes
○ No

Primary question answered Yes

1. Please provide the auditor a copy of the Incident Response Training material.

☐ I have read and will comply.

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented please provide the auditor a copy of the Incident Response Training material.

☐ I have read and will comply.

3. IR-4 INCIDENT HANDLING

Has the agency implemented:

a. An incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;
b. Coordinates incident handling activities with contingency planning activities;
c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly; and
d. Ensures the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization?

Control Enhancements:

(1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES
Does the agency 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?

○ Yes
○ No

4. IR-5 INCIDENT MONITORING

Does the agency track and document incidents?

NOTE: Can the agency provide details on previous incidents over the previous year.

Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics as well as evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports. IR-4 provides information on the types of incidents that are appropriate for monitoring.

○ Yes
○ No

5. IR-6 INCIDENT REPORTING

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

(1) INCIDENT REPORTING | AUTOMATED REPORTING

Does the agency report incidents using automated mechanisms?

NOTE: The recipients of incident reports are specified in IR-6b. Automated reporting mechanisms include email, posting on websites (with automatic updates), and automated incident response tools and programs.

○ Yes
○ No

6. IR-7 INCIDENT RESPONSE ASSISTANCE

Has the agency provided 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.

NOTE: Incident response support resources provided by organizations include help desks, assistance groups, automated ticketing systems to open and track incident response tickets, and access to forensics services or consumer redress services, when required.

○ Yes
○ No

7. Please acknowledge the agency has reviewed the CJIS Security Policy (CJISSECPOL) version 5.9.3 and is fully aware of the security controls within the IR-INCIDENT RESPONSE section that are sanctionable for audit beginning October 1, 2024.

☐ I have read and understand the above statement.

Section - Policy Area 4 - Auditing and Accountability (AU)

1. AU-2 EVENT LOGGING & AC-2(4)

Does the agency 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);
b. 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;
c. Specify the following event types for logging within the system:
All successful and unsuccessful:
1. System log-on attempts
2. Attempts to use:
a. Access permission on a user account, file, directory, or other system resource;
b. Create permission on a user account, file, directory, or other system resource;
c. Write permission on a user account, file, directory, or other system resource;
d. Delete permission on a user account, file, directory, or other system resource;
e. Change permission on a user account, file, directory, or other system resource.
3. Attempts to change account passwords
4. Actions by privileged accounts (i.e., root, Oracle, DBA, admin, etc.)
5. Attempts for users to:
a. Access the audit log file;
b. Modify the audit log file;
c. Destroy the audit log file.
d. 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
e. Review and update the event types selected for logging annually.

○ Yes
○ No

2. AU-3 CONTENT OF AUDIT RECORDS

Does the agency ensure that audit records contain information that establishes the following:
a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

AU-3 (1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION

a. Session, connection, transaction, and activity duration;
b. Source and destination addresses;
c. Object or filename involved; and
d. Number of bytes received and bytes sent (for client-server transactions) in the audit records for audit events identified by type, location, or subject.
e. The III portion of the log shall clearly identify:
1. The operator
2. The authorized receiving agency
3. The requestor
4. The secondary recipient

○ Yes
○ No

Primary question answered Yes

1. Please provide the auditor a SIEM (System Information & Event Management) tool report that shows activities and logging conducted by an employee(s) and/or vendor(s) during a specific time period within the past year that demonstrate the event types and content of the audit records.

Please keep in mind, this also applies to agency-owned Live Scan devices.

○ Yes
○ No

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented please provide the auditor a SIEM (System Information & Event Management) tool report that shows activities and logging conducted by an employee(s) and/or vendor(s) during a specific time period within the past year that demonstrate the event types and content of the audit records.

Please keep in mind, this also applies to agency-owned Live Scan devices.

☐ I have read and will comply.

3. AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES

Does the agency,
a. 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
b. Take the following additional actions: restart all audit logging processes and verify system(s) are logging properly.

○ Yes
○ No

4. AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

Does the agency,
a. Review and analyze system audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity;
b. Report findings to organizational personnel with audit review, analysis, and reporting responsibilities and organizational personnel with information security and privacy responsibilities; and
c. 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.

○ Yes
○ No

5. AU-8 TIME STAMPS

Does the agency,
a. Use internal system clocks to generate time stamps for audit records;
b. 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.

○ Yes
○ No

6. AU-9 PROTECTION OF AUDIT INFORMATION

Does the agency,
a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and
b. 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.

○ Yes
○ No

7. AU-11 AUDIT RECORD RETENTION

Does the agency,
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.

○ Yes
○ No

8. Please acknowledge the agency has reviewed the CJIS Security Policy (CJISSECPOL) version 5.9.4 and is fully aware of the security controls within the AU-AUDIT AND ACCOUNTABILITY section that are sanctionable for audit beginning October 1, 2024.

☐ I have read and understand the above statement.

Section - Policy Area 5 - Access Control (AC)

1. AC-2 ACCOUNT MANAGEMENT, AC-3 ACCESS ENFORCEMENT, AC-5 SEPARATION OF DUTIES, AC-6 LEAST PRIVILEGE & 5.12.2 & 3 PERSONNEL TERMINATION AND TRANSFER

Does the agency:

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;
b. Assign account managers;
c. Require conditions for group and role membership;
d. Specify:
1. Authorized users of the system;
2. Group and role membership
e. Require approvals by organizational personnel with account management responsibilities for requests to create accounts;
f. Create, enable, modify, disable, and remove accounts in accordance with agency policy;
g. Monitor the use of accounts;
i. Authorize access to the system based on:
1. A valid access authorization;
2. Intended system usage
j. Review accounts for compliance with account management requirements at least annually;
k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
l. Align account management processes with personnel termination and transfer processes.

○ Yes
○ No

2. AC-6 (1) AUTHORIZE ACCESS TO SECURITY FUNCTIONS

Does the agency 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:
(a) Established system accounts, configured access authorizations (i.e., permissions, privileges), set events to be audited, set intrusion detection parameters, and other security functions; and
(b) Security-relevant information in hardware, software, and firmware.

○ Yes
○ No

3. AC-6 (2) NON-PRIVILEGED ACCESS FOR NON-SECURITY FUNCTIONS

Does the agency 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?

○ Yes
○ No

Primary question answered Yes

1. Please provide the auditor an account list showing all users that have privileged access, what roles provide the user privileged access, and the associated non-privileged account assigned to the individual.

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented please provide the auditor an account list showing all users that have privileged access, what roles provide the user privileged access, and the associated non-privileged account assigned to the individual.

☐ I have read and will comply.

4. AC-6 (5) PRIVILEGED ACCOUNTS

Does the agency restrict privileged accounts on the system to privileged users?

○ Yes
○ No

5. AC-6 (7) LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES

Does the agency:

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

○ Yes
○ No

6. AC-6 (9) LOG USE OF PRIVILEGED FUNCTIONS

Does the agency log the execution of privileged functions?

○ Yes
○ No

7. AC-6 (10) PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

Does the agency prevent non-privileged users from executing privileged functions?

○ Yes
○ No

8. AC-7 UNSUCCESSFUL LOGON ATTEMPTS

Does the agency:
a. Enforce a limit of five (5) consecutive invalid logon attempts by a user during a 15-minute time period; and
b. Automatically lock the account or node until released by an administrator when the maximum number of unsuccessful attempts is exceeded?

○ Yes
○ No

9. AC-8 SYSTEM USE NOTIFICATION

Does the system 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:
1. Users are accessing a restricted information system;
2. System usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
4. Use of the system indicates consent to monitoring and recording;
b. 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; and
c. For publicly accessible systems:
1. 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;
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system?

○ Yes
○ No

Primary question answered Yes

1. Please provide a screenshot of each system use notification and state if applied at the system or application level. If at application level, please provide the name of the application(s).

☐ I have read and will comply.

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented please provide a screenshot of each system use notification and state if applied at the system or application level. If at application level, please provide the name of the application(s).

☐ I have read and will comply.

10. AC-11 DEVICE LOCK

Does the information system accessing CJI:

a. Prevent further access to the system by initiating a device lock after a maximum of 30 minutes of inactivity and requiring the user to initiate a device lock before leaving the system unattended.
NOTE: In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) 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.
b. Retain the device lock until the user reestablishes access using established identification and authentication procedures?

NOTE 1: This includes any connected device(s) including MBIS, Live Scan, and ULW.
NOTE 2: Exemptions; MDT's (Patrol Vehicles), Dispatch, and Receive Only Terminals (ROT).

○ Yes
○ No

11. AC-11 (1) PATTERN-HIDING DISPLAYS

Does the information system conceal, via the device lock, information previously visible on the display with a publicly viewable image?

NOTE: In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) 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.

Please be prepared to show the auditor how this is configured at the system level.

○ Yes
○ No

12. AC-17 REMOTE ACCESS

Has the agency:

a. Established and documented usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b. Authorized each type of remote access to the system prior to allowing such connections?

In addition, please verify that the following Control Enhancements have been implemented.

(1) REMOTE ACCESS | MONITORING AND CONTROL
Control:
Employ automated mechanisms to monitor and control remote access methods.

(2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION
Control:
Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

(3) REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS
Control:
Route remote accesses through authorized and managed network access control points.

(4) REMOTE ACCESS | PRIVILEGED COMMANDS AND ACCESS
Control:
a. 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 the following needs: compelling operational needs; and
b. Document the rationale for remote access in the security plan for the system.

NOTE: 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.

This control includes any connected device(s) including MBIS, Live Scan, and ULW.

○ Yes
○ No

Primary question answered Yes

1. Please provide your auditor a copy of the agency remote access policy and 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 units, 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.

NOTE: An explanation of how the required controls are being met should be included in either the agency remote access policy or the documented step-by-step procedures.
(1) NOTE: Audit logging for remote access is enforced by AU-2. Audit events are defined in AU-2a.
(3) NOTE: Organizations consider the Trusted Internet Connections (TIC) initiative requirements for external network connections since limiting the number of access control points for remote access reduces attack surfaces.
https://www.cisa.gov/resources-tools/programs/trusted-internet-connections-tic
(4) NOTE: 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.

☐ I have read and will comply.

2. Please define the cryptographic mechanisms the agency has implemented to protect the confidentiality and integrity of remote access sessions.

NOTE: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.

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented Please provide your auditor a copy of the agency remote access policy and 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 units, 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.

NOTE: An explanation of how the required controls are being met should be included in either the agency remote access policy or the documented step-by-step procedures.
(1) NOTE: Audit logging for remote access is enforced by AU-2. Audit events are defined in AU-2a.
(3) NOTE: Organizations consider the Trusted Internet Connections (TIC) initiative requirements for external network connections since limiting the number of access control points for remote access reduces attack surfaces.
https://www.cisa.gov/resources-tools/programs/trusted-internet-connections-tic
(4) NOTE: 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.

NOTE: Be prepared to define the cryptographic mechanisms the agency has implemented to protect the confidentiality and integrity of remote access sessions.

☐ I have read and will comply.

13. AC-18 WIRELESS ACCESS

Does the agency:

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and
b. Authorize each type of wireless access to the system prior to allowing such connections?

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. AC-18 (3) WIRELESS ACCESS | DISABLE WIRELESS NETWORKING

Does the agency disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment?

NOTE: Wireless networking capabilities that are embedded within system components represent a significant potential vulnerability that can be exploited by adversaries. Disabling wireless capabilities when not needed for essential organizational missions or functions can reduce susceptibility to threats by adversaries involving wireless technologies.

○ Yes
○ No

14. AC-18 (1) WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION

Does the agency protect wireless access to the system using authentication of authorized users and agency-controlled devices, and encryption?

○ Yes
○ No

15. AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Has the agency:

a. Established configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and
b. Authorize the connection of mobile devices to organizational systems.

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. Please provided the auditor confirmation the agency is meeting the technical controls required for mobile devices. In regard to mobile devices with a limited feature operating systems, this is typically done using Mobile Device Management (CJISSECPOL 5.13.2).

NOTE: A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile device functionality may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones and tablets. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of notebook/desktop systems, depending on the nature and intended purpose of the device. 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. Controlled areas are spaces for which organizations provide physical or procedural controls to meet the requirements established for protecting information and systems. Due to the large variety of mobile devices with different characteristics and capabilities, organizational restrictions may vary for the different classes or types of such devices. Usage restrictions and specific implementation guidance for mobile devices include configuration management, device identification and authentication, implementation of mandatory protective software, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware.
Usage restrictions and authorization to connect may vary among organizational systems. For example, the organization may authorize the connection of mobile devices to its network and impose a set of usage restrictions, while a system owner may withhold authorization for mobile device connection to specific applications or impose additional usage restrictions before allowing mobile device connections to a system. Adequate security for mobile devices goes beyond the requirements specified in AC-19. Many safeguards for mobile devices are reflected in other controls. AC-20 addresses mobile devices that are not organization-controlled.

2. AC-19(5) ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE OR CONTAINER-BASED ENCRYPTION

Please provide the auditor confirmation that any areas in which CJI may be stored on the mobile device are encrypted. This is typically done using Windows Bitlocker.

NOTE: 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.

☐ I have read and will comply.

16. AC-20 USE OF EXTERNAL SYSTEMS

Has the agency:
a. Established 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
b. 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.

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. AC-20 (1) USE OF EXTERNAL SYSTEMS | LIMITS ON AUTHORIZED USE

Does the agency:

Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:
a. 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
b. Retention of approved system connection or processing agreements with the organizational entity hosting the external system?

○ Yes
○ No

17. AC-20 (2) USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES — RESTRICTED USE

Does the agency restrict the use of organization-controlled portable storage devices by authorized individuals on external systems?

NOTE: Limits on the use of organization-controlled portable storage devices in external systems include restrictions on how the devices may be used and under what conditions the devices may be used.

○ Yes
○ No

18. AC-21 INFORMATION SHARING

Does the agency:

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions as defined in an executed information exchange agreement; and
b. 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?

○ Yes
○ No

19. Please acknowledge the agency has reviewed the CJIS Security Policy (CJISSECPOL) version 5.9.4 and is fully aware of the security controls within the AC-ACCESS CONTROL section that are sanctionable for audit beginning October 1, 2024.

☐ I have read and understand the above statement.

Section - Policy Area 6 - Identification and Authentication (IA)

1. 5.6 IDENTIFICATION AND AUTHENTICATION (IA)
IA-0 USE OF ORIGINATING AGENCY IDENTIFIERS IN TRANSACTIONS AND INFORMATION EXCHANGES

Is the agency ensuring that an FBI authorized originating agency identifier (ORI) is used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction? The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.

○ Yes
○ No

2. IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Does the agency uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of users to ensure detailed accountability of individual activity?

○ Yes
○ No

3. IA-4 IDENTIFIER MANAGEMENT

Does the agency manage system identifiers by:

a. Receiving authorization from organizational personnel with identifier management responsibilities to assign an individual, group, role, service, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, service, or device;
c. Assigning the identifier to the intended individual, group, role, service, or device?

○ Yes
○ No

4. IA-5 AUTHENTICATOR MANAGEMENT

Does the agency manage system authenticators by:

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; and
g. Protecting authenticator content from unauthorized disclosure and modification.

○ Yes
○ No

5. IA-5(1) AUTHENTICATOR MANAGEMENT | AUTHENTICATOR TYPES

Please select all of the Authenticator Types currently in use by the agency:

Below is a list of the current CJISSECPOL security controls for the specific authenticator types:

(a) Memorized Secret Authenticators and Verifiers:
(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;
(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.

☐ (a) Memorized Secret Authenticators and Verifiers
☐ (b) Look-up Secrets 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)

6. IA-5(2) AUTHENTICATOR MANAGEMENT | PUBLIC KEY-BASED AUTHENTICATION

Does the agency utilize public key-based authentication or public key infrastructure (PKI)?

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. Does the agency:
(a) For public key-based authentication:
1. Enforce authorized access to the corresponding private key; and
2. Map the authenticated identity to the account of the individual or group; and
(b) When public key infrastructure (PKI) is used:
1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
2. Implement a local cache of revocation data to support path discovery and validation.

○ Yes
○ No

7. IA-5(6) AUTHENTICATOR MANAGEMENT| PROTECTION OF AUTHENTICATORS

Does the agency:

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

NOTE: For systems that contain multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems. Security categories of information are determined as part of the security categorization process.

○ Yes
○ No

8. Please acknowledge the agency has reviewed the CJIS Security Policy (CJISSECPOL) version 5.9.4 and is fully aware of the security controls within the IA-IDENTIFICATION AND AUTHENTICATION section that are sanctionable for audit beginning October 1, 2024.

☐ I have read and understand the above statement.

Section - Policy Area 7 - Configuration Management

1. 5.7.1.2 Network Diagram

Does the agency have a current Network Diagram which includes the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. “For Official Use Only” (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.

Please provide the auditor a current agency network diagram and include an equipment list that details the following for all devices on the network diagram: Make, Model, Current Installed O/S or Firmware version, Latest O/S or Firmware Version Available, Date Last Updated, End of Support Date.

NOTE: The Configuration Management control family has just been updated by the APB and was released 0n 7.23.2024 in the CJISSECPOL version 5.9.5.

○ Yes
○ No

Primary question answered Yes

1. Please send the auditor a current (updated) agency network diagram for review. Please also include an equipment list of all agency equipment on the network diagram, detailing the equipment Make, Model, OS/Firmware Version, Date Last Updated, End of Support Date.

☐ I have read and will comply.

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented please send the auditor a current (updated) agency network diagram for review.
Please also include an equipment list of all agency equipment on the network diagram, detailing the equipment Make, Model, OS/Firmware Version, Date Last Updated, End of Support Date.

☐ I have read and will comply.

Section - Policy Area 8 - Media Protection (MP)

1. MP-1 POLICY AND PROCEDURES

1. Does the agency have documented media protection policy that has been disseminated to authorized individuals that:
(a) addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
(b) is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Has the agency documented procedures to facilitate the implementation of the media protection policy and the associated media protection controls, and have these procedures been disseminated to authorized individuals; and
b. Has the agency designated an individual with security responsibilities to manage the development, documentation, and dissemination of the media protection policy and procedures?
c. Does the agency Review and update the current media protection:
1. Policy at least annually and following any security incidents involving digital and/or non-digital media; and
2. Procedures at least annually and following any security incidents involving digital and/or non-digital media.

○ Yes
○ No

Primary question answered Yes

1. Please provide the auditor a copy of the agency's documented Media Protectoin Policy and a copy of the agency's step-by-step procedures.

☐ I have read and will comply.

2. How does the agency validate authorized individuals acknowledge the policy/procedures?

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented, please provide the auditor a copy of the agency's documented Media Protection Policy and a copy of the agency's step-by-step procedures.

☐ I have read and will comply.

2. MP-2 MEDIA ACCESS

Does the agency restrict access to digital and non-digital media to authorized individuals?

○ Yes
○ No

Primary question answered Yes

1. Please explain how this control is met in the Media Protection Step-by-Step Procedures.

NOTE: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Denying access to hard copies of case file information stored in a locked filing cabinet is an example of restricting access to non-digital media. Limiting access to the design specifications stored on compact discs in the media library to individuals on the system development team is an example of restricting access to digital media.

☐ I have read and will comply.

3. MP-4 MEDIA STORAGE

Does the agency physically control and securely store digital and non-digital media within physically secure locations or controlled areas and encrypt CJI on digital media when physical and personnel restrictions are not feasible; and protect system digital and non-digital media until the media are destroyed or sanitized using approved equipment, techniques, and procedures?

○ Yes
○ No

Primary question answered Yes

1. Please explain how this control is met in the Media Protection Step-by-Step Procedures.

NOTE: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Physically controlling stored media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the library, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a controlled media library.

☐ I have read and will comply.

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented, Please explain how this control is met in the Media Protection Step-by-Step Procedures.

NOTE: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Physically controlling stored media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the library, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a controlled media library.

☐ I have read and will comply.

4. MP-5 MEDIA TRANSPORT

Does the agency protect and control digital (flash drives, external hard drives) and non-digital media (micro-film, paper) to help prevent compromise of the data during transport outside of the physically secure locations or controlled areas using encryption; and restrict the activities associated with transport of system, electronic, and physical media to authorized personnel maintaining accountability for system media during transport outside of the physically secure location or controlled areas; and documents the activities associated with the transport of system media?

○ Yes
○ No

Primary question answered Yes

1. Please explain how this control is met in the Media Protection Step-by-Step Procedures.

NOTE: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state and magnetic), compact discs, and digital versatile discs. Non-digital media includes microfilm and paper. Controlled areas are spaces for which agencies provide physical or procedural controls to meet requirements established for protecting information and systems. Controls to protect media during transport include cryptography and locked containers. Cryptographic mechanisms can provide confidentiality and integrity protections depending on the mechanisms implemented. Activities associated with media transport include releasing media for transport, ensuring that media enters the appropriate transport processes, and the actual transport. Authorized transport and courier personnel may include individuals external to the agency. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and/or obtaining records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering.

☐ I have read and will comply.

Primary question answered No

1. This is a requirement of the CJISSSECPOL.
Once implemented, Please explain how this control is met in the Media Protection Step-by-Step Procedures.

NOTE: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state and magnetic), compact discs, and digital versatile discs. Non-digital media includes microfilm and paper. Controlled areas are spaces for which agencies provide physical or procedural controls to meet requirements established for protecting information and systems. Controls to protect media during transport include cryptography and locked containers. Cryptographic mechanisms can provide confidentiality and integrity protections depending on the mechanisms implemented. Activities associated with media transport include releasing media for transport, ensuring that media enters the appropriate transport processes, and the actual transport. Authorized transport and courier personnel may include individuals external to the agency. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and/or obtaining records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering.

☐ I have read and will comply.

5. MP-6 MEDIA SANITIZATION

Does the agency:

a. 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. Inoperable digital media will be destroyed (cut up, shredded, etc.). Physical media will be securely disposed of when no longer needed for investigative or security purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration; and
b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information?

○ Yes
○ No

Primary question answered Yes

1. Please explain how this control is met in the Media Protection Step-by-Step Procedures.

NOTE: Media sanitization applies to all digital and non-digital system media subject to disposal or reuse, whether or not the media is considered removable. Examples include digital media in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media (e.g., paper and microfilm). The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed. Sanitization techniques—including clearing, purging, cryptographic erase, de-identification of personally identifiable information, and destruction—prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Agencies determine the appropriate sanitization methods, recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization.
Agencies use discretion on the employment of approved sanitization techniques and procedures for media that contains information deemed to be in the public domain or publicly releasable or information deemed to have no adverse impact on agencies or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document.

☐ I have read and will comply.

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented, please explain how this control is met in the Media Protection Step-by-Step Procedures.

NOTE: Media sanitization applies to all digital and non-digital system media subject to disposal or reuse, whether or not the media is considered removable. Examples include digital media in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media (e.g., paper and microfilm). The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed. Sanitization techniques—including clearing, purging, cryptographic erase, de-identification of personally identifiable information, and destruction—prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Agencies determine the appropriate sanitization methods, recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization.
Agencies use discretion on the employment of approved sanitization techniques and procedures for media that contains information deemed to be in the public domain or publicly releasable or information deemed to have no adverse impact on agencies or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing a classified appendix from an otherwise unclassified document, or redacting

selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document.

☐ I have read and will comply.

6. MP-7 MEDIA USE

Does the agency:

a. 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 (examples below); and
b. 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
c. 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?

○ Yes
○ No

7. Please acknowledge the agency has reviewed the CJIS Security Policy (CJISSECPOL) version 5.9.4 and is fully aware of the security controls within the MP-MEDIA PROTECTION section that are sanctionable for audit beginning October 1, 2024.

☐ I have read and understand the above statement.

Section - Policy Area 9 - Physical Protection (PE)

1. PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Does the agency,
a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;
b. Issue authorization credentials for facility access;
c. Review the access list detailing authorized facility access by individuals annually and when personnel changes occur; and
d. Remove individuals from the facility access list when access is no longer required.

○ Yes
○ No

Primary question answered Yes

1. Please provide the auditor a list of authorized personnel, including vendors, subcontractors, etc.

NOTE: Physical access authorizations apply to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include ID badges, identification cards, and smart cards. Physical access authorizations may not be necessary to access certain areas within facilities that are designated as publicly accessible.

☐ I have read and will comply.

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented, please the auditor a list of authorized personnel, including vendors, subcontractors, etc.

NOTE: Physical access authorizations apply to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include ID badges, identification cards, and smart cards. Physical access authorizations may not be necessary to access certain areas within facilities that are designated as publicly accessible.

☐ I have read and will comply.

2. PE-3 PHYSICAL ACCESS CONTROL

Does the agency,
a. Enforce physical access authorizations by:
1. Verifying individual access authorizations before granting access to the facility; and
2. Controlling ingress and egress to the facility using agency-implemented procedures and controls;
b. Maintain physical access audit logs for the physically secure location and agency-defined sensitive areas;
c. 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;
d. Escort visitors and control visitor activity in all physically secure locations;
e. Secure keys, combinations, and other physical access devices;
f. Inventory all agency-issued physical access devices annually; and
g. Change combinations and keys when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.
h. If the above conditions cannot be met refer to the requirements listed in PE-17.

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. Please ensure the auditor is shown how the agency meets this requirement.

NOTE: 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 determine the types of guards needed, including professional security staff, system users, or administrative staff. Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical access control systems comply with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. 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.

☐ I have read and will comply.

Primary question answer 2 selected

1. This is a requirement of the CJISSECPOL.
Once implemented, please ensure the auditor is shown how the agency meets this requirement.

NOTE: 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 determine the types of guards needed, including professional security staff, system users, or administrative staff. Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical access control systems comply with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. 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.

☐ I have read and will comply.

Primary question answer 3 selected

1. Please explain the agency "N/A" response.

3. PE-4 ACCESS CONTROL FOR TRANSMISSION

Does the agency control physical access to information system distribution and transmission lines and devices within organizational facilities using agency-implemented procedures and controls?

○ Yes
○ No

Primary question answered Yes

1. Please ensure the auditor is shown how the agency meets this requirement.

NOTE: 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.

☐ I have read and will comply.

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented, please ensure the auditor is shown how the agency meets this requirement.

NOTE: 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.

☐ I have read and will comply.

4. PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

Does the agency control physical access to output from monitors, printers, scanners, audio devices, facsimile machines, and copiers to prevent unauthorized individuals from obtaining the output.

○ Yes
○ No

Primary question answered Yes

1. Please ensure the auditor is shown how the agency meets this requirement.

NOTE: Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and allowing access to authorized individuals only, placing output devices in locations that can be monitored by personnel, installing monitor or screen filters, and using headphones. Examples of output devices include monitors, printers, scanners, audio devices, facsimile machines, and copiers.

Please check the Live Scan device in the Jail Booking Area. it should not be facing a holding cell. Even if this is new jail construction, the Live Scan screen should prevent unauthorized individuals from obtaining the output.

The same goes for the Desk Duty Officer greeting the public, and the Records areas where I have heard comments from the public stating "I have a better booking photo that that" as the individual was looking at the records clerk's computer monitor through the glass partition separting the public from the records department.

The previous CJISSECPOL terminology was "viewable", the new CJISSECPOL terminology is "prevent unauthorized individuals from obtaining the output." I mention this simply because it does not say anything about not being able to read the contents on the screen. The fact is, the unauthorized individual should not even be able to see the screen.

☐ I have read and will comply.

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented, please ensure the auditor is shown how the agency meets this requirement.

NOTE: Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and allowing access to authorized individuals only, placing output devices in locations that can be monitored by personnel, installing monitor or screen filters, and using headphones. Examples of output devices include monitors, printers, scanners, audio devices, facsimile machines, and copiers.

Please check the Live Scan device in the Jail Booking Area. it should not be facing a holding cell. Even if this is new jail construction, the Live Scan screen should prevent unauthorized individuals from obtaining the output.

The same goes for the Desk Duty Officer greeting the public, and the Records areas where I have heard comments from the public stating "I have a better booking photo that that" as the individual was looking at the records clerk's computer monitor through the glass partition separting the public from the records department.

The previous CJISSECPOL terminology was "viewable", the new CJISSECPOL terminology is "prevent unauthorized individuals from obtaining the output." I mention this simply because it does not say anything about not being able to read the contents on the screen. The fact is, the unauthorized individual should not even be able to see the screen.

☐ I have read and will comply.

5. PE-6 MONITORING PHYSICAL ACCESS

Does the agency,
a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;
b. 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
c. Coordinate results of reviews and investigations with the organizational incident response capability.

○ Yes
○ No

6. PE-6 (1) MONITORING PHYSICAL ACCESS | INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT

Does the agency monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment?

○ Yes
○ No

7. PE-17 ALTERNATE WORK SITE

Does the agency,
a. Determine and document all alternate facilities or locations allowed for use by employees;
b. Employ the following controls at alternate work sites:
1. Limit access to the area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
2. Lock the area, room, or storage container when unattended.
3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
4. Follow the encryption requirements found in SC-13 and SC-28 for electronic storage (i.e., data at-rest) of CJI.
c. Assess the effectiveness of controls at alternate work sites; and
d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. Please provide the auditor blank copies of all alternate work site agreements, such as telecommute agreements. Please ensure these areas are noted on the agency network diagram as alternate work locations and if there are numerous locations please only identify the quantity of each, based upon the unique methods of connectivity.

NOTE: 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.

☐ I have read and will comply.

Primary question answer 2 selected

1. This is a requirement of the CJISSECPOL.
Once implemented, please provide the auditor blank copies of all alternate work site agreements, such as telecommute agreements. Please ensure these areas are noted on the agency network diagram as alternate work locations and if there are numerous locations please only identify the quantity of each, based upon the unique methods of connectivity.

NOTE: 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.

☐ I have read and will comply.

Primary question answer 3 selected

1. Please explain the "N/A" response?

8. Please acknowledge the agency has reviewed the CJIS Security Policy (CJISSECPOL) version 5.9.4 and is fully aware of the security controls within the PE-PHYSICAL PROTECTION section that are sanctionable for audit beginning October 1, 2024.

☐ I have read and understand the above statement.

Section - Policy Area 10: Systems and Communications Protection (SC)

1. SC-2 SEPARATION OF SYSTEM AND USER FUNCTIONALITY

Does the agency separate user functionality, including user interface services, from system management functionality?

○ Yes
○ No

2. SC-7 BOUNDARY PROTECTION

Does the agency,
a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnets for publicly accessible system components that are physically or logically separated from internal organizational networks; and
c. 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.

○ Yes
○ No

Primary question answered Yes

1. Please ensure the agency network diagram accurately depicts the established boundary protection.

NOTE: Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture. Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs.
Restricting or prohibiting interfaces within organizational systems includes restricting external web traffic to designated web servers within managed interfaces, prohibiting external traffic that appears to be spoofing internal addresses, and prohibiting internal traffic that appears to be spoofing external addresses.
[SP 800-189] provides additional information on source address validation techniques to prevent ingress and egress of traffic with spoofed addresses. Commercial telecommunications services are provided by network components and consolidated management systems shared by customers. These services may also include third party-provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions.
Boundary protection may be implemented as a common control for all or part of an organizational network such that the boundary to be protected is greater than a system-specific boundary (i.e., an authorization boundary).

○ Yes
○ No

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented, please ensure the agency network diagram accurately depicts the established boundary protection.

NOTE: Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture. Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs.
Restricting or prohibiting interfaces within organizational systems includes restricting external web traffic to designated web servers within managed interfaces, prohibiting external traffic that appears to be spoofing internal addresses, and prohibiting internal traffic that appears to be spoofing external addresses.
[SP 800-189] provides additional information on source address validation techniques to prevent ingress and egress of traffic with spoofed addresses. Commercial telecommunications services are provided by network components and consolidated management systems shared by customers. These services may also include third party-provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions.
Boundary protection may be implemented as a common control for all or part of an organizational network such that the boundary to be protected is greater than a system-specific boundary (i.e., an authorization boundary).

☐ I have read and will comply.

3. SC - 7(8) BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS

Does the agency 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?

○ Yes
○ No

4. SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY & AC-4 INFORMATION FLOW ENFORCEMENT

Does the agency 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.

○ Yes
○ No

Primary question answered Yes

1. Please provide the auditor copies of enrollment agreements for agency cloud-based solutions ensuring the Cloud Service Provider and/or Software as a Service (SaaS) solution provider is not using any derived metadata for commercial or advertising purposes.

NOTE: Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as any system components that can transmit information, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of information can be accomplished by physical or logical means. Physical protection can be achieved by using protected distribution systems. A protected distribution system is a wireline or fiber-optics telecommunications system that includes terminals and adequate electromagnetic, acoustical, electrical, and physical controls to permit its use for the unencrypted transmission of classified information. Logical protection can be achieved by employing encryption techniques. Organizations that rely on commercial providers who offer transmission services as commodity services rather than as fully dedicated services may find it difficult to obtain the necessary assurances regarding the implementation of needed controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality or integrity services are available in standard, commercial telecommunications service packages. If it is not feasible to obtain the necessary controls and assurances of control effectiveness through appropriate contracting vehicles, organizations can implement appropriate compensating controls. The agency may permit limited use of metadata derived from unencrypted CJI when specifically approved by the agency and its “intended use” is detailed within the service agreement. Such authorized uses of metadata may include but are not limited to the following: spam and spyware filtering, data loss prevention, spillage reporting, transaction logs (events and content–similar to the AU controls), data usage/indexing metrics, and diagnostic/syslog data.

○ Yes
○ No

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented please provide the auditor copies of enrollment agreements for agency cloud-based solutions ensuring the Cloud Service Provider and/or Software as a Service (SaaS) solution provider is not using any derived metadata for commercial or advertising purposes.

NOTE: Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as any system components that can transmit information, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of information can be accomplished by physical or logical means. Physical protection can be achieved by using protected distribution systems. A protected distribution system is a wireline or fiber-optics telecommunications system that includes terminals and adequate electromagnetic, acoustical, electrical, and physical controls to

permit its use for the unencrypted transmission of classified information. Logical protection can be achieved by employing encryption techniques. Organizations that rely on commercial providers who offer transmission services as commodity services rather than as fully dedicated services may find it difficult to obtain the necessary assurances regarding the implementation of needed controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality or integrity services are available in standard, commercial telecommunications service packages. If it is not feasible to obtain the necessary controls and assurances of control effectiveness through appropriate contracting vehicles, organizations can implement appropriate compensating controls. The agency may permit limited use of metadata derived from unencrypted CJI when specifically approved by the agency and its “intended use” is detailed within the service agreement. Such authorized uses of metadata may include but are not limited to the following: spam and spyware filtering, data loss prevention, spillage reporting, transaction logs (events and content–similar to the AU controls), data usage/indexing metrics, and diagnostic/syslog data.

☐ I have read and will comply.

5. SC-8 (1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION

○ Yes
○ No

6. SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Does the agency 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?

○ Yes
○ No

7. SC-13 CRYPTOGRAPHIC PROTECTION

Does the agency,
a. Determine the use of encryption for CJI in-transit when outside a physically secure location; and
b. 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.

○ Yes
○ No

Primary question answered Yes

1. To validate the certification status, please provide the auditor a copy of all FIPS 140-3 certificates, downloaded from the NIST website below:

https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search

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.

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented please provide the auditor a copy of all FIPS 140-3 certificates,which can be downloaded from the NIST website below:

https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search

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.

☐ I have read and will comply.

8. SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Does the agency,
a. Issue public key certificates under an agency-level certificate authority or obtain public key certificates from an approved service provider; and
b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

NOTE: 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.

○ Yes
○ No
○ N/A

9. SC-28 PROTECTION OF INFORMATION AT REST

Does the agency 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).

NOTE: DPS has enhanced this requirement and limited the permitted cloud environments to DPS approved government cloud environments.

Note: 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).

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. SC-28 (1) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION

Does the agency implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on information systems and digital media outside physically secure locations: CJI?

NOTE: The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category or classification of the information. Organizations have the flexibility to encrypt information on system components or media or encrypt data structures, including files, records, or fields.

○ Yes
○ No

10. Please acknowledge the agency has reviewed the CJIS Security Policy (CJISSECPOL) version 5.9.4 and is fully aware of the security controls within the SC-SYSTEMS AND COMMUNICATIONS PROTECTION section that are sanctionable for audit beginning October 1, 2024.

☐ I have read and understand the above statement.

Section - Policy Area 11 - Formal Audits

1. 5.11.1.2 Triennial Security Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs.

Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.

5.11.2 Audits by the CSA

Each CSA shall:
1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies.
3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
4. Have the authority, on behalf of another CSA, to conduct a CSP compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.

☐ I have read and understand the above statement.

Section - Policy Area 12 - Personnel Security

1. 5.12 Personnel Security

Have all personnel who access CJIS data either physically, logically, or remotely been fingerprint based background checked, by the agency prior to being granted access?

○ Yes
○ No

2. 5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI

Does the agency maintain a list of personnel who have been authorized unescorted access to unencrypted CJI?

○ Yes
○ No

Primary question answered Yes

1. Please provide the auditor a current copy of the access list.

☐ I have read and will comply.

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented please provide the auditor a current copy of the access list.

☐ I have read and will comply.

3. 5.12.4 Personnel Sanctions

Does the agency have a formal sanctions process for personnel failing to comply with established information security policies and procedures?

○ Yes
○ No

Primary question answered Yes

1. Please email a copy of local policy which reflects personnel sanctions processes to your auditor for review.

☐ I have read and will comply.

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented please email a copy of local policy which reflects personnel sanctions processes to your auditor for review

☐ I have read and will comply.

Section - Policy Area 13 - Mobile Devices

1. 5.13 Mobile Devices

Has the agency established written usage restrictions and implementation guidelines for wireless technologies? (ex: BYOD policy or local SOP, MDM Policy).

○ YES
○ NO
○ NA

Primary question answer 1 selected

1. Please ensure a copy of the local policy or SOP is provided to your auditor for review.

☐ I have read and will comply.

2. 5.13.1.1 All 802.XX Wireless Protocols

If applicable, has the agency implemented the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:

1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.

2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.

3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.

4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.

5. Enable user authentication and encryption mechanisms for the management interface of the AP.

6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Section 5.6.2.1.

7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.

8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.

9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.

10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.

11. Ensure that the ad hoc mode has been disabled.

12. Disable all non essential management protocols on the APs.

13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.

14. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.

15. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between

wireless networks and the wired network to only operational needs.

16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

○ YES
○ NO
○ NA

3. 5.13.1.4 Mobile Hotspots

If applicable, does the agency allow mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, meet at a minimum configuration:

1. Enable encryption on the hotspot

2. Change the hotspot's default SSID

a. Ensure the hotspot SSID does not identify the device make/model or agency ownership

3. Create a wireless network password (Pre-shared key)

4. Enable the hotspot's port filtering/blocking features if present

5. Only allow connections from agency controlled devices

○ YES
○ NO
○ NA

4. 5.13.2 Mobile Device Management (MDM)

If Mobile Device Management (MDM) is in use, does it meet at a minimum the following compensating controls:

Remote locking of device

Remote wiping of device

Setting and locking device configuration

Detection of "rooted" or "jailbroken" devices

Enforce folder and/or disk level encryption

Application of mandatory policy settings on the device

Detection of unauthorized configurations

Detection of unauthorized software or applications

Ability to determine the location of agency controlled devices

Prevention of unpatched devices from accessing CJI or CJI systems

Automatic device wiping after a specified number of failed attempts

○ YES
○ NO
○ NA

Primary question answer 1 selected

1. Provide details below regarding type and software solution in use for MDM.

5. 5.13.3 Wireless Device Risk Mitigations

If applicable, utilizing wireless devices - Has the agency established at a minimum the following risk controls:

1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1
2. Are configured for local device authentication (see Section 5.13.7.1)
3. Use Advanced Authentication or CSO approved compensating controls as per Section 5.13.7.2.1
4. Encrypt all CJI resident on the device.
5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.
6. Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.

○ Yes
○ No
○ N/A

6. 5.13.4.3 Personal Firewall

A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems).

Does the firewall, at a minimum, perform the following activities?

1. Manage program access to the Internet.

2. Block unsolicited requests to connect to the user device.

3. Filter incoming traffic by IP address or protocol.

4. Filter incoming traffic by destination ports.

5. Maintain an IP traffic log.

○ YES
○ NO
○ NA

Primary question answer 1 selected

1. Please provide brief description of Firewall solution in place.

(IE; Built-in Windows firewall, software name, etc.)

7. 5.13.5 Incident Response (Mobile Devices)

In addition to the requirements in Section 5.3 Incident Response, agencies are responsible to meet additional reporting and handling procedures.

Has the agency developed a written plan which includes special reporting procedures for mobile devices in any of the following situations?

1. Loss of device control. For example:

a. Device known to be locked, minimal duration of loss

b. Device lock state unknown, minimal duration of loss

c. Device lock state unknown, extended duration of loss

d. Device known to be unlocked, more than momentary duration of loss

2. Total loss of device

3. Device compromise

4. Device loss or compromise outside the United States

○ YES
○ NO
○ NA

Primary question answer 1 selected

1. Please provide (if not already submitted) a copy of the agency's Incident Response Plan which covers mobile devices (Handhelds / Tablets) to your auditor.

☐ I have read and will comply.

8. 5.13.7.2 Advanced Authentication

When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user unless the access to CJI is indirect as described in Section 5.6.2.2.1. If access is indirect, then AA is not required.

Is Advanced Authentication (AA) in use?

○ YES
○ NO
○ NA

Primary question answer 1 selected

1. Provide software solution and details of what AA solution is in place at the agency below.

Section - Policy Area 14 - System and Services Acquisition (SA)

1. SA-22 UNSUPPORTED SYSTEM COMPONENTS

Does the agency:

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or
b. Provide the following options for alternative sources for continued support for unsupported components: original manufacturer support, or original contracted vendor support?

This is why we request the End of Support Date on the Equipment List as part of the Agency Network Diagram.

NOTE: Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components. 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.
Alternative sources for support address the need to provide continued support for system components that are no longer supported by the original manufacturers, developers, or vendors when such components remain essential to organizational mission and business functions. If necessary, organizations can establish in-house support by developing customized patches for critical software components or, alternatively, obtain the services of external providers who provide ongoing support for the designated unsupported components through contractual relationships. Such contractual relationships can include open-source software value-added vendors. 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.

○ Yes
○ No

2. Please acknowledge the agency has reviewed the CJIS Security Policy (CJISSECPOL) version 5.9.4 and is fully aware of the security controls within the SA-SYSTEM AND SERVICES ACQUISITION section that are sanctionable for audit beginning October 1, 2024.

☐ I have read and understand the above statement.

Section - Policy Area 15 - System and Information Integrity (SI)

1. SI-1 POLICY AND PROCEDURES

Does the agency:

a. Develop, document, and disseminate to all organizational personnel with system and information integrity responsibilities and information system owners:
1. Agency-level system and information integrity policy that:
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;
b. Designate organizational personnel with system and information integrity responsibilities to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and
c. Review and update the current system and information integrity:
1. Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and
2. Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI?

○ Yes
○ No

Primary question answered Yes

1. Please provide the auditor a copy of the agency's documented System and Information Integrity Policy and Step-By-Step Procedures.

NOTE: System and information integrity policy and procedures address the controls in the SI family that are implemented within systems and organizations.
The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and information integrity policy and procedures.
Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.
Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed.
Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.
Events that may precipitate an update to system and information integrity policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

☐ I have read and will comply.

2. How does the agency validate authorized individuals acknowledge the policy/procedures?

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented please provide the auditor a copy of the agency's documented System and Information Integrity Policy and Step-By-Step Procedures.

NOTE: System and information integrity policy and procedures address the controls in the SI family that are implemented within systems and organizations.
The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and information integrity policy and procedures.
Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.
Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed.
Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.
Events that may precipitate an update to system and information integrity policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

☐ I have read and will comply.

2. SI-2 FLAW REMEDIATION

Does the agency:

a. Identify, report, and correct system flaws;
b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation
c. 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

d. Incorporate flaw remediation into the organizational configuration management process?

The auditors will randomly assess agency systems to confirm they are kept current.

NOTE: The need to remediate system flaws applies to all types of software and firmware. Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities.
Security-relevant updates include patches, service packs, and malicious code signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified.
Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of risk factors, including the security category of the system, the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw), the organizational risk tolerance, the mission supported by the system, or the threat environment.
Some types of flaw remediation may require more testing than other types. Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed.
In some situations, organizations may determine that the testing of software or firmware

updates is not necessary or practical, such as when implementing simple malicious code signature updates.
In testing decisions, organizations consider whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

○ Yes
○ No

3. SI-2 (2) FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS

Does the agency 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?

○ Yes
○ No

Primary question answered Yes

1. Please provide the auditor the Name, Version, and physical location of the agency scanning tool used to meet this requirement and be prepared to demonstrate status on select systems.

NOTE: Automated mechanisms can track and determine the status of known flaws for system components.

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once Implemented, please provide the auditor the Name, Version, and physical location of the agency scanning tool used to meet this requirement and be prepared to demonstrate status on select systems.

☐ I have read and will comply.

4. SI-3 MALICIOUS CODE PROTECTION
Please provide the auditor the Name, Version, and physical location of the agency Malicious Code Protection software used to meet this requirement and be prepared to demonstrate status on select systems.

a. Implement signature-based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; .
b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;
c. 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; and
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; and
d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

NOTE: System entry and exit points include firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices.
Malicious code includes viruses, worms, Trojan horses, and spyware.
Malicious code can also be encoded in various formats contained within compressed or hidden files or hidden in files using techniques such as steganography.

Malicious code can be inserted into systems in a variety of ways, including by electronic mail, the World Wide Web, and portable storage devices.

5. SI-4 SYSTEM MONITORING

The agency shall:

a. Monitor the information system to detect:
1. Attacks and indicators of potential attacks.
2. Unauthorized local, network, and remote connections.
b. Identify unauthorized use of the information system through defined techniques and methods.
c. Deploy monitoring devices strategically within the information system to collect [entity determined essential information] and at ad hoc locations within the system to track specific types of transactions of interest to the entity.
d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
e. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to operations and assets, individuals, other organizations, or based on law enforcement information, intelligence information, or other credible sources of information.
f. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable state and federal laws, directives, policies, or regulations.
g. Provide information system monitoring information to authorized personnel or business units as needed.

○ Yes
○ No

Primary question answered Yes

1. Please provide the auditor the Name, Version, and physical location of the agency systems used to meet this requirement and demonstrate status on select systems.

NOTE: Depending on the security architecture, the distribution and configuration of monitoring devices may impact throughput at key internal and external boundaries as well as at other locations across a network due to the introduction of network throughput latency. If throughput management is needed, such devices are strategically located and deployed as part of an established organization-wide security architecture.
Strategic locations for monitoring devices include selected perimeter locations and near key servers and server farms that support critical applications. Monitoring devices are typically employed at the managed interfaces associated with controls SC-7 and AC-17. The information collected is a function of the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies.
Adjustments to levels of system monitoring are based on law enforcement information, intelligence information, or other sources of information. The legality of system monitoring activities is based on applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

☐ I have read and will comply.

Primary question answered No

1. This is a requirement of the CJISSECPOL.
Once implemented please provide the auditor the Name, Version, and physical location of the agency systems used to meet this requirement and demonstrate status on select systems.

NOTE: Depending on the security architecture, the distribution and configuration of monitoring devices may impact throughput at key internal and external boundaries as well as at other locations across a network due to the introduction of network throughput latency. If throughput management is needed, such devices are strategically located and deployed as part of an established organization-wide security architecture.
Strategic locations for monitoring devices include selected perimeter locations and near key servers and server farms that support critical applications. Monitoring devices are typically employed at the managed interfaces associated with controls SC-7 and AC-17. The information collected is a function of the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies.
Adjustments to levels of system monitoring are based on law enforcement information, intelligence information, or other sources of information. The legality of system monitoring activities is based on applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

☐ I have read and will comply.

6. SI-4 (2) SYSTEM MONITORING | AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS

Does the agency employ automated tools and mechanisms to support real-time analysis of events, such as Security Information and Event Management (SIEM) technologies?

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. Please provide the auditor the Name, Version, and physical location of the agency additional tools used to meet this requirement and be prepared to demonstrate status on select systems.

NOTE: 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.
Automated monitoring techniques can create unintended privacy risks because automated controls may connect to external or otherwise unrelated systems.
The matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

☐ I have read and will comply.

Primary question answer 2 selected

1. This is a requirement of the CJISSECPOL.
Once implemented please provide the auditor the Name, Version, and physical location of the agency additional tools used to meet this requirement and be prepared to demonstrate status on select systems.

NOTE: 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.
Automated monitoring techniques can create unintended privacy risks because automated controls may connect to external or otherwise unrelated systems.
The matching of records between these systems may create linkages with unintended

consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

☐ I have read and will comply.

Primary question answer 3 selected

1. Please explain the reason for the N/A response:

7. SI-4 (4) SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

Does the agency:
a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
b. 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?

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. Please provide the auditor the Name, Version, and physical location of the agency additional tools used to meet this requirement and be prepared to demonstrate status on select systems.

NOTE: Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic includes internal traffic that indicates 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. Evidence of malicious code or unauthorized use of legitimate code or credentials is used to identify potentially compromised systems or system components.

☐ I have read and will comply.

Primary question answer 2 selected

1. This is a requirement of the CJISSECPOL.
Once implemented please provide the auditor the Name, Version, and physical location of the agency additional tools used to meet this requirement and be prepared to demonstrate status on select systems.

NOTE: Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic includes internal traffic that indicates 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. Evidence of malicious code or unauthorized use of legitimate code or credentials is used to identify potentially compromised systems or system components.

☐ I have read and will comply.

Primary question answer 3 selected

1. Please explain the reason for the N/A response:

8. SI-4 (5) SYSTEM MONITORING | SYSTEM-GENERATED ALERTS

Does the agency alert organizational personnel with system monitoring responsibilities when the following system generated indications of compromise or potential compromise occur: inappropriate or unusual activities with security or privacy implications?

NOTE: Alerts may be generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. In contrast to alerts generated by the system, alerts generated by organizations in SI-4(12) focus on information sources external to the system, such as suspicious activity reports and reports on potential insider threats.

○ Yes
○ No
○ N/A

Primary question answer 3 selected

1. Please explain the reason for the N/A response:

9. SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Does the agency:
a. Receive system security alerts, advisories, and directives from external source(s) (e.g., CISA, Multi-State Information Sharing & Analysis Center [MS-ISAC], U.S. Computer Emergency Readiness Team [USCERT], hardware/software providers, federal/state advisories, etc.) on an ongoing basis;
b. Generate internal security alerts, advisories, and directives as deemed necessary;
c. Disseminate security alerts, advisories, and directives to: organizational personnel implementing, operating, maintaining, and using the system

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. Please provide the auditor a list of active agency subscriptions meeting SI-5 a of this requirement and attest to appropriate dissemination.

NOTE: The Cybersecurity and Infrastructure Security Agency (CISA) generates security alerts and advisories to maintain situational awareness throughout the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives.
Compliance with security directives is essential due to the critical nature of many of these directives and the potential (immediate) adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner.
External organizations include supply chain partners, external mission or business partners, external service providers, and other peer or supporting organizations.

In addition, it is highly recommended the agency LASO subscribe to the DPS CJIS Security Office Technical Listserv

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

also available at

https://www.dps.texas.gov/section/crime-records/welcome-tx-cjis-security-office

Primary question answer 2 selected

1. This is a requirement of the CJISSECPOL.
Once implemented please provide the auditor a list of active agency subscriptions meeting SI-5 a of this requirement and attest to appropriate dissemination.

NOTE: The Cybersecurity and Infrastructure Security Agency (CISA) generates security alerts and advisories to maintain situational awareness throughout the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives.
Compliance with security directives is essential due to the critical nature of many of these directives and the potential (immediate) adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner.
External organizations include supply chain partners, external mission or business partners, external service providers, and other peer or supporting organizations.

In addition, it is highly recommended the agency LASO subscribe to the DPS CJIS Security Office Technical Listserv

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

also available at

https://www.dps.texas.gov/section/crime-records/welcome-tx-cjis-security-office

☐ I have read and will comply.

Primary question answer 3 selected

1. Please explain the reason for the N/A response:

10. SI-8 SPAM PROTECTION

Is the agency meeting all the controls for both SI-8 & SI-8(2) listed below?

a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and
b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

SI-8(2) SPAM PROTECTION | AUTOMATIC UPDATES

Control:
Automatically update spam protection mechanisms at least daily.

NOTE: Using automated mechanisms to update spam protection mechanisms helps to ensure that updates occur on a regular basis and provide the latest content and protection capabilities.

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. Please provide the auditor the Name, Version, and physical location of the agency tool(s) used to meet this requirement and be prepared to demonstrate status on select systems.

NOTE: System entry and exit points include firewalls, remote-access servers, electronic mail servers, web servers, proxy servers, workstations, notebook computers, and mobile devices. Spam can be transported by different means, including email, email attachments, and web accesses. Spam protection mechanisms include signature definitions.

Primary question answer 2 selected

1. This is a requirement of the CJISSECPOL.
Once implemented please provide the auditor the Name, Version, and physical location of the agency tool(s) used to meet this requirement and be prepared to demonstrate status on select systems.

NOTE: System entry and exit points include firewalls, remote-access servers, electronic mail servers, web servers, proxy servers, workstations, notebook computers, and mobile devices. Spam can be transported by different means, including email, email attachments, and web accesses. Spam protection mechanisms include signature definitions.

☐ I have read and will comply.

Primary question answer 3 selected

1. Please explain the reason for the N/A response:

11. SI-11 ERROR HANDLING

How are error messages being generated that provide the information necessary for corrective actions without revealing information that could be exploited and are you ensuring that these messages are only being revealed to organizational personnel with security responsibilities?

12. SI-12 INFORMATION MANAGEMENT AND RETENTION

Does the agency 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?

○ Yes
○ No
○ N/A

Primary question answer 3 selected

1. Please explain the reason for the N/A response:

13. Please acknowledge the agency has reviewed the CJIS Security Policy (CJISSECPOL) version 5.9.4 and is fully aware of the security controls within the SI-SYSTEM AND INFORMATION INTEGRITY section that are sanctionable for audit beginning October 1, 2024.

☐ I have read and understand the above statement.