CJIS Technical Audit 5.9.5 v2.0

Preview

Report created: Wed Apr 08 2026 16:49:37 GMT-0500 (Central Daylight Time)

Section - Agency Information

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

CJIS Documents | Department of Public Safety

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.

Data derived from TLETS 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., Data derived from TLETS) 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 of agency designated organizational personnel:

3.2.3 Terminal Agency Coordinator (TAC)

3.2.9 Local Agency Security Officer (LASO) - Organizational Personnel with Security Responsibilities (OPSR)

3. Please select all entities that support the agency in processing, storing, or transmitting Criminal Justice Information (CJI), including but not limited to IT service providers.

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

4. Please select all that apply from the list below if the agency is being hosted or is hosting services for other agencies.

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

5. Please list the agency name which hosts or provides your agency access to TLETS.

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

7. How does the agency process, store, and/or transmit CJI?

☐ OpenFox
☐ CAD
☐ RMS
☐ Cloud-based Systems
☐ Other (JMS, Livescan, Court Systems, License Plate Reader)

8. Please provide a comprehensive list below of all applications used by the agency to process, transmit, and/or store Criminal Justice Information (CJI), and indicate whether the agency has direct or indirect access to CJI for each application.

9. Does the agency access Texas Law Enforcement Telecommunications System (TLETS) using wired and/or wireless devices (e.g., desktops, laptops, mobile data terminals (MDTs), tablets, or mobile phones)?

○ Yes
○ No

Primary question answered Yes

1. If yes, indicate the device types and provide the total number of devices for each:

Wired devices (desktops, docking stations, etc.)

Total number of wired devices used to access TLETS: _____

Wireless devices (MDTs, laptops, tablets, mobile phones, etc.)

Total number of wireless devices used to access TLETS: _____

10. Is the agency utilizing biometric identification systems, such as:

Live Scan - Fingerprint/IRIS capture system that can be purchased from Idemia or about seven other vendors on the FBI website as meeting fingerprint capture requirements. The FBI listing does not mean these devices are CJIS compliant, it means the device meets FBI print capture criteria only.

ULW - Universal Latent Workstation - This is software provided by the FBI that could be on many different systems. The fingerprint is collected/lifted and shared through a central location; returns are not directly sent back to the computer that sent the information.

MBIS (Multimodal Biometric Identification System) - The MBIS is controlled by DPS. MBIS is an application running on a PC with a full-featured OS. MBIS appears as an icon on the desktop and opens as Integra ID with a prompt for a separate User ID and password. MBIS falls under a contract with vendor NEC that is housed at DPS where the servers are located.

Mobile ID is a portable fingerprint capture device connecting to a laptop/tablet device. Captures typically one or two prints via a direct cable or Bluetooth to main laptop or tablet. The agency uses a store and forward method to transmit the prints to the DPS as a pass through to the FBI via a SFTP connection. DPS takes the encrypted SFTP, decrypts the record and transmits to the FBI. DPS acts as the pass through for the record. Mobile ID works in conjunction with MBIS as a quick print capture.

○ Yes
○ No

Primary question answered Yes

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

2. Are these fingerprint devices routed through another agency? If so, please specify.

Section - Policy Area 1 - Information Exchange Agreements

1. 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.

(Example dissemination to court, Victim Notifications, Email.....etc.)

2. Please list any vendors that share CJI with outside agencies or entities?

2. 5.1.1.4 Management Control Agreements

Does the agency have a Management Control Agreement for all non-law enforcement governmental entities providing criminal justice services/support for the agency?

Requirement (CJIS):

A Management Control Agreement (MCA) is required whenever a non criminal justice governmental entity (NCJA) supports or performs functions affecting CJIS systems or CJI on behalf of a criminal justice agency (CJA). The MCA ensures "management control of the criminal justice function remains solely with the Criminal Justice Agency." (CJIS Security Policy § 5.1.1.4, Appendix D 2)

Evidence examples (agency can provide):

- **Signed MCA between the CJA and the NCJA (current and in force).**
- **Scope statement showing the NCJA's services (e.g., network/IT support) and CJA authority over priorities, personnel access, operations, and security.**

• List of NCJA personnel with logical/physical access to CJI and their vetting status (to show the CJA oversees access control).

○ Yes
○ No
○ N/A

Primary question answer 1 selected

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

☐ I have read and will comply.

3. 5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum

Does the agency have a signed Security Addendum for each vendor or subcontractor that provides CJIS system support or has unescorted access to secure agency locations?

Requirement (CJIS):

Any private contractor with access to CJIS systems/CJI or unescorted access to secure areas must execute the FBI CJIS Security Addendum, acknowledging responsibilities across personnel, site, system, data, and technical security. Agencies must retain signed acknowledgments for audit. (https://www.dps.texas.gov/SecurityReview/SecurityAddendum.doc)

Evidence examples:

• A vendor list with corresponding signed CJIS Security Addendum Certification page acknowledgments (each contractor staff member).

• Contract language referencing the CJIS Security Addendum and compliance with the current CJIS policy version.

• Background checks/adjudication records for vendor personnel with CJI access (where applicable by state policy).

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. If applicable, please provide a copy of each fully executed Security Addendum to the auditor. Ensure that these agreements are maintained and updated to reflect any vendor personnel changes.

☐ I have read and will comply.

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

1. AT-3 ROLE-BASED TRAINING
[Existing] [Priority 2]

Have all personnel (including Dispatchers, Law Enforcement, IT staff, and Contractors) received appropriate role-based CJIS Security and Privacy Training?

CJIS Requirement:

CJIS Security Policy § 5.2 Security Awareness Training requires that all personnel with access to CJI complete role-based training at initial access and at intervals defined by the policy (prior to access and once a year afterwards). Training must be tailored to the individual's role (e.g., terminal operator, IT admin, contractor) to ensure they understand responsibilities and risks.

Evidence Examples:

- Training curriculum mapped to CJIS roles (Dispatcher, LE, IT, Contractor).
- Completion records showing initial and annually training dates for each user.
- Learning Management Systems (LMS) or manual logs demonstrating role-specific modules were assigned and completed

○ Yes
○ No

2. AT-4 TRAINING RECORDS
[Existing] [Priority 4]

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

CJIS Requirement:

CJIS § 5.2 mandates that agencies maintain documentation of training completion for audit purposes. The policy, along with state CJIS program requirements and FBI audit guidance, requires agencies to retain at least three years of records to demonstrate compliance across audit cycles.

Evidence Examples:

- Archived Learning Management System (LMS) reports or spreadsheets showing training dates and completion status for all personnel.
- Signed certificates or acknowledgment forms stored in personnel files.
- Policy stating retention period for training records (≥ three years).

○ Yes
○ No

Section - Policy Area 3 - Incident Response (IR)

1. IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES
[Existing] [Priority 2]

Has the agency developed and documented an Incident Response Policy and Procedures?

CJIS Requirement:

CJIS Security Policy § 5.3 Incident Response requires agencies to develop, document, and implement incident response capabilities. This includes defining responsibilities, reporting requirements, and escalation paths for suspected or confirmed security incidents involving CJI.

Evidence Examples:

- **A formal Incident Response Policy approved by agency leadership.**
- **Procedures detailing incident categories, reporting timelines, and roles/responsibilities.**
- **References to CJIS requirements in the policy (e.g., notification to CSA/FBI).**

○ Yes
○ No

Primary question answered Yes

1. Please provide a copy of the documented Incident Response Policy and Procedures to the auditor.

Confirm that the policy includes the following elements:

Report to DPS contact ETOC (previously known as OIC) 1-888-DPS-OICO (1-888-377-6420).
Roles and responsibilities
Incident reporting process
Response and recovery steps
Testing and review schedule

☐ I have read and will comply.

2. IR-5 INCIDENT MONITORING

Does the agency track and document incidents?

CJIS Requirement:

CJIS § 5.3 requires agencies to track, document, and maintain records of security incidents for accountability and audit purposes. Documentation should include incident type, date/time, actions taken, and resolution.

Evidence Examples:

• Incident log or ticketing system entries showing incident details and resolution steps.
• Reports summarizing incidents for management review.
• Retention policy for incident records (typically ≥ 3 years).

○ Yes
○ No

Primary question answered Yes

1. If yes, how does the agency track and document incidents?
(Examples: Incident tracking system, ticketing software, manual logs, spreadsheets, etc.)

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

1. AU-1 POLICY AND PROCEDURES
[Existing] [Priority 1]

Has the agency developed, approved, and maintained a documented policy and step-by-step procedures that define roles, responsibilities, and how audit logging and reviews are conducted?

CJIS Requirement:

Maintain an agency/system level audit & accountability policy and detailed procedures; designate personnel with audit responsibilities; review/refresh at least annually and after security incidents.

Evidence Examples:

- Signed Audit & Accountability Policy with revision date ≤ 12 months.
- SOPs for event logging, review cadence, escalation, and retention.
- Designation letters (OPSR/ISO/TAC/LASO) showing audit responsibilities.

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. How does the agency validate that all authorized individuals have acknowledged the policy and procedures, and what evidence is maintained to demonstrate compliance?

2. Please provide the auditor with a copy of the agency's documented Audit and Accountability Policy, the step-by-step procedures for audit logging and review.

☐ I have read and will comply.

2. AU-2/3 EVENT LOGGING & CONTENT REVIEW
[Priority 1 – DPS Enhanced Priority 1]

Does the agency have documented processes and technical controls to:
a. Identify which system activities must be logged and coordinate with other departments (such as IT or Investigations) to ensure important events are captured; and

b. Ensure audit records include the following information:

• What type of event occurred

• When the event occurred

• Where the event occurred

• The source of the event

• The outcome of the event

• The identity of any individuals or entities associated with the event?

CJIS Requirement (AU-2):

Define event types to log and coordinate with stakeholders; log successful/failed logons, access/use, privilege changes, and operational transactions sufficient to reconstruct activities.

Evidence Examples:

• SIEM/on host logging profile listing the events collected.
• Platform configs (e.g., Windows Advanced Auditing, Linux audit, DB logs).
• Data flow map showing log sources and ingest to SIEM.

CJIS Requirement (AU-3):

Include user identity, timestamp, event source, type/action, and outcome in audit records to enable accountability.

Evidence Examples:
Sample logs showing required fields for authentication and access events. Parser/normalization rules in SIEM mapping fields consistently.

○ 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.

☐ I have read and will comply.

3. AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES
[Existing] [Priority 1]

Does the agency:
a. Detect and alert designated personnel (e.g., audit and accountability staff, system/network administrators) within one (1) hour of any audit logging process failure, including stoppage or inability to write logs?

b. Take corrective actions, including:
• Restarting all affected audit logging processes
• Verifying that logging has resumed and is functioning properly
• Documenting the incident and resolution steps

CJIS Requirement:

Detect and respond to logging failures—generate alerts, switch to fail safe/alternative logging, and restore normal operations promptly.

Evidence Examples:

• Alert rules (e.g., no events received alarms).
• Tickets showing incident handling for logging outages.

○ Yes
○ No

4. AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING
[Existing] [Priority 1]

Does the agency:
a. Review and analyze audit logs at least once per week to identify unusual or unauthorized access/activity?
b. Notify appropriate personnel if audit logs show suspicious or inappropriate system access?
c. Adjust the frequency of log reviews based on changes in risk (e.g., law enforcement intel, incidents, alerts)?
d. Document and report findings to the designated security officer or management as required by policy?

CJIS Requirement:

Perform regular log review/analysis/reporting, with defined cadence, responsibilities, and response procedures.

Evidence Examples:

- Weekly/monthly review reports; case notes for anomalies.
- Metrics on alert closure time; trend reports to leadership.

○ Yes
○ No

5. AU-9 PROTECTION OF AUDIT INFORMATION
[Existing] [Priority 1]

Does the agency:
a. Implement technical and administrative controls to protect audit information and audit logging tools from unauthorized access, modification, and deletion?
b. Restrict access to audit logs and tools to authorized personnel only?
c. Alert designated personnel (audit/accountability staff, information security/privacy officers, system/network administrators) upon detection of any unauthorized access, modification, or deletion of audit information?
d. Document and report any such incidents as required by policy?

CJIS Requirement:

Implement controls to protect audit information, including role based access, separation of duties, and tamper resistance.

Evidence Examples:
- SIEM/admin RBAC; write once storage (e.g., immutable buckets).
- Change control for log pipelines/collectors.

○ Yes
○ No

6. AU-11 AUDIT RECORD RETENTION
[Existing] [Priority 1]

Does the agency:
a. Retain audit records for a minimum of one (1) year, or longer if required for administrative, legal, audit, or operational purposes?
b. Store retained audit records securely to prevent unauthorized access, modification, or deletion?
c. Document retention and disposal procedures in accordance with CJIS Security Policy?

CJIS Requirement:

The agency shall retain audit records for an agency-defined retention period sufficient to support incident investigations, operational needs, and CJIS audit activities. Audit records must be retained for at least one (1) year, or longer if required for administrative, legal, audit, or operational purposes, in accordance with the CJIS Security Policy.

Some agencies elect to retain logs for multiple years to support triennial CJIS audit cycles, though this is an organizational decision rather than a CJIS policy requirement.

Evidence Examples:

- Retention schedule; storage tier configs; aging policy in SIEM.
- Proof of retrieval for historical investigations.

○ Yes
○ No

Section - Policy Area 5 - Access Control (AC)

1. AC-2 ACCOUNT MANAGEMENT
AC-2 Account Management Enhanced Controls (3), (5), (13)
[Existing] [Priority 1]

Does the agency have documented account management processes that:

1. Define and control account types and access
- Specify allowed/prohibited account types, authorized users, roles, and privileges.
- Require documented approvals before account creation or changes.

2. Manage the account lifecycle
• Create, modify, disable, and remove accounts promptly based on HR events (termination, transfer, role changes).
• Align with personnel processes and enforce timely disablement (within one business day).

3. Monitor and review accounts
• Detect and alert on account anomalies or unauthorized activity.
• Respond quickly to account issues and disable accounts immediately when no longer needed.
• Conduct periodic reviews (at least annually) to confirm compliance.

4. Secure shared/group accounts
• Rotate authenticators when membership changes or eliminate shared accounts where possible.

CJIS Requirement:

1. Define and enforce access control
Agencies must define account types, roles, privileges, and enforce documented approvals for account creation and modification (CJIS §5.5).

Evidence Examples:
• Access Control Policy listing account types and roles
• Approved account creation/change forms or workflow logs

2. Manage the account lifecycle
CJIS Requirement: Accounts must be created, modified, disabled, and removed promptly, with disablement ideally within one business day of separation or role change.
Evidence Examples:
• HR–IT workflow documentation
• Logs showing account disablement aligned with termination dates

3. Monitor and review accounts
CJIS Requirement: Agencies must monitor account activity for anomalies and conduct periodic (at least annual) access reviews.
Evidence Examples:
• SIEM alerts for unusual account activity
• Annual access review reports with sign off

4. Secure shared/group accounts
CJIS Requirement: Shared accounts should be avoided; if used, authenticators must be rotated whenever membership changes.
Evidence Examples:
• Policy prohibiting or restricting shared accounts
• Logs showing password changes after membership updates

○ Yes
○ No

2. AC-4 INFORMATION FLOW ENFORCEMENT
[Existing] [Priority 1]

Does the agency enforce controls that ensure information only flows through authorized and protected paths by preventing unencrypted CJI from being sent across public networks, blocking external traffic that attempts to appear as internal agency traffic, and ensuring that all outbound web requests are routed only through approved agency-managed boundary protection devices such as firewalls, proxies, gateways, or routers?

CJIS Requirement:

The agency must enforce approved authorizations governing the flow of Criminal Justice Information (CJI) within the system and between connected systems. Controls must prevent the transmission of unencrypted CJI across public networks, block external traffic impersonating internal agency traffic, and ensure all outbound web requests to the public network pass only through agency-controlled boundary protection devices such as proxies, gateways, firewalls, or routers.

Status: Existing requirement, Priority 1

Evidence Examples:

Policy or SOP defining:
• Requirements to encrypt all CJI before transmitting it across public or untrusted networks.
• Procedures to block or inspect inbound traffic that improperly claims an internal agency source.
• Mandates that all externally facing web requests must be routed through agency-controlled boundary devices (e.g., proxy servers, firewalls, gateways, routers).
• Criteria for approving any exceptions and associated compensating controls.

Boundary Protection Device Configurations:
• Screenshots or configuration exports from firewalls, proxies, or gateways showing rules blocking inbound spoofed traffic and forcing all outbound web requests through approved paths.
• Encryption settings confirming enforcement of secure transmission for CJI (e.g., TLS requirements, VPN configurations).
• Network diagrams highlighting internal systems, boundary devices, and approved information flow paths.

Monitor Logs and Traffic Inspection Records:
• Network or traffic logs showing blocked traffic that violates flow control policies (e.g., spoofed headers, unapproved ports).
• Alert logs from intrusion detection/prevention systems (IDS/IPS) indicating attempts to transmit unencrypted CJI or bypass boundary devices.
• Web proxy logs showing validation that outbound requests originate only from agency-controlled sources.

System Security Plan (SSP):
• Sections describing AC 4 information flow controls, boundary devices in use, encryption enforcement, and network architecture.
• Explanation of traffic inspection mechanisms and rule enforcement processes.

Change Management and Oversight Records:
• Change tickets or approvals for updates to boundary protection configurations or encryption enforcement controls.
• Review logs or audit trails confirming periodic validation and testing of flow control mechanisms.

○ Yes
○ No

3. AC-6 (2) NON-PRIVILEGED ACCESS FOR NON-SECURITY FUNCTIONS
AC-6 (5) PRIVILEGED ACCOUNTS
[Existing] [Priority 1]

Does the agency enforce least privilege by:

• Restricting access rights to the minimum necessary for job functions?
• Requiring privileged users to use non-privileged accounts for routine activities?
• Conducting periodic reviews of privileged accounts and access rights?

CJIS Requirement:

CJIS Security Policy § 5.5 Access Control mandates:

• Least Privilege: Users must have only the access necessary for their duties.
• Privileged Account Management: Admins must use non-privileged accounts for day-to-day tasks and only elevate when needed.
• Periodic Reviews: Agencies must review privileged accounts regularly (at least annually) to confirm appropriateness.

Evidence Examples:

• Access Control Policy explicitly stating least privilege and separate admin accounts.
• Screenshots or reports showing dual accounts for admins (one standard, one privileged).
• Privileged Access Management (PAM) logs or review reports.
• Annual access review documentation with sign-off.

○ Yes
○ No

Primary question answered Yes

1. Please provide:

1. A complete list of all users with privileged access, including:
• Username
• Associated privileged roles or permissions
• System(s) where privileges apply

2. The corresponding non-privileged account assigned to each privileged user.

3. A list of non-privileged accounts used for routine, non-security functions (e.g., email, standard applications).

☐ I have read and will comply.

4. AC-7 UNSUCCESSFUL LOGON ATTEMPTS
[Existing] [Priority 1]

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?

CJIS Requirement:

CJIS Security Policy § 5.5 Access Control requires agencies to implement technical controls that:

- Limit consecutive invalid logon attempts to five within 15 minutes.
- Lock the account or system after the threshold is reached, requiring manual administrator intervention to restore access.

This is a Priority 1 control in the CJIS Requirements Companion and is considered an existing requirement (already enforceable in audits).

Evidence Examples:

- Group Policy Object (GPO) or system configuration screenshots showing:
- Account lockout threshold = 5 attempts.
- Reset counter after 15 minutes.
- Lockout duration = until admin unlocks.
- Test results or logs showing lockout behavior after failed attempts.
- Policy documentation referencing these settings.

○ Yes
○ No

5. AC-8 SYSTEM USE NOTIFICATION
[Existing] [Priority 1]

Does each system display an approved system use notification banner before granting access, and does the banner include required elements (authorized use, monitoring consent, and consequences of misuse)?

CJIS Requirement:

CJIS Security Policy § 5.5 Access Control requires that all systems providing access to CJI display a System Use Notification (banner) prior to granting access. The banner must include:

- Authorized Use Statement (system for official use only).
- Monitoring Consent (user consents to monitoring).
- Consequences of Misuse (violations may result in disciplinary action or criminal prosecution).

This is an existing requirement and marked Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

- Screenshot of the login banner from each system (CJIS-compliant wording).
- Policy specifying banner content and enforcement.
- Configuration settings (e.g., GPO for Windows, SSH banner for Linux, VPN portal banner).

○ Yes
○ No

Primary question answered Yes

1. Indicate whether the banner is applied at the system level or application level

○ System Level
○ Application Level
○ Both

2. If applied at the application level, provide the name(s) of the application(s) where the banner is displayed.

3. Provide a screenshot of the system use notification banner for each system.

☐ I have read and will comply.

6. AC-11 DEVICE LOCK
[Existing] [Priority 4]

Does the agency configure and enforce device lock settings so that information systems automatically lock after no more than 30 minutes of inactivity, require users to manually lock their devices when left unattended, and ensure locked devices can only be unlocked through the agency's established identification and authentication procedures?

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.

CJIS Requirement:

Agencies must ensure that all devices used to access, process, or transmit Criminal Justice Information (CJI) automatically initiate a device lock after no more than 30 minutes of inactivity, require users to manually lock their devices when left unattended, and retain the device lock until the user successfully reauthenticates through the agency's approved identification and authentication mechanisms. These controls must be consistently applied across all CJI-authorized workstations, laptops, mobile devices, and terminals, except for devices formally exempted under CJIS policy (e.g., dispatch consoles in physically secure and continuously staffed locations).

Status: Existing requirement, Priority 4

Evidence Examples:

Policy or SOP defining:
• Device lock timeout requirements (≤30 minutes of inactivity).
• Requirement for users to initiate a manual device lock when leaving devices unattended.
• Rules for systems eligible for CJIS approved exemptions (e.g., dispatch, conveyance systems, receive only terminals).
• Reauthentication requirements and approved methods (password, MFA, smart card, etc.).
• Responsibilities for monitoring compliance (IT/security administrators, supervisors, etc.).

Device Configuration Records:
• Endpoint management system screenshots or exports showing lock timeout settings.
• Mobile device management (MDM) policies detailing inactivity lock enforcement.
• Desktop/laptop configuration baselines reflecting CJIS aligned password/lock settings.
• Technical documentation confirming lock state persists until reauthentication.

Compliance Monitoring Evidence:
• Log reviews documenting device lock enforcement or violations.
• Spot check records showing verification of manually locked devices.
• Help desk tickets showing remediation of misconfigured lock settings.
• Reports from configuration compliance tools (e.g., SCCM, Intune, JAMF).

System Security Plan (SSP):
• Sections describing AC 11 implementation: auto lock timeout, manual lock procedures, reauthentication requirements, and exemptions.
• Diagrams or narratives explaining how device lock controls are enforced on various device types (workstations, laptops, MDTs, mobile devices).

○ Yes
○ No

Primary question answered Yes

1. AC-11 (1) PATTERN-HIDING DISPLAYS
[Existing] [Priority 4]

When a device is locked, does the system hide any sensitive information that was previously visible on the screen (e.g., replacing it with a generic lock screen image)?

CJIS Requirement:

CJIS Security Policy § 5.5 Access Control requires that when a device is locked, sensitive information must not remain visible. The system should display a generic lock screen or similar mechanism to prevent unauthorized viewing of CJI or other sensitive data.

Status: Existing control (Priority 4 in the Requirements Companion, but enforceable now).

Evidence Examples:

• Screenshots showing the lock screen hides all application content (Windows, macOS, mobile devices).
• MDM or GPO configuration enforcing lock screen behavior.
• Policy stating devices must obscure sensitive information when locked.

○ Yes
○ No

7. AC-17 REMOTE ACCESS
[Existing] [Priority 1]

Does the agency have documented policies and procedures for remote access that:

- **Define usage restrictions and configuration requirements for each type of remote access (e.g., VPN, RDP)?**
- **Require formal authorization before enabling any remote access method?**

CJIS Requirement:

CJIS Security Policy § 5.5 Access Control requires agencies to:

- **Establish remote access policies and procedures that define acceptable methods (VPN, RDP, etc.), configuration standards, and security requirements.**
- **Require formal authorization before enabling any remote access capability.**
- **Ensure remote access is secured with encryption and advanced authentication (MFA) and is monitored and logged.**

This is an existing requirement and marked Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

- **Documented Remote Access Policy specifying allowed methods, configuration standards, and security controls.**
- **Approval workflow or forms showing authorization before enabling remote access.**
- **VPN/RDP configuration screenshots showing MFA and encryption settings.**
- **Logs demonstrating remote access sessions are monitored.**

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. Please provide:

1. A copy of the agency's Remote Access Policy.

2. Documented step-by-step procedures for each remote access method used to connect to the agency's secure network or systems that process CJI.

This includes:
• Agency units
• Remote workers
• IT support staff
• Vendors or contractors

Note: If anyone connects from outside an agency secure location to the agency secure network, they are using remote access. Include all methods currently in use or planned for use.

☐ I have read and will comply.

2. (1) REMOTE ACCESS | MONITORING AND CONTROL
[Existing] [Priority 1]

Does the agency employ automated mechanisms to monitor and control remote access methods.

CJIS Requirement:

CJIS Security Policy § 5.5 Access Control requires agencies to:

- Implement automated mechanisms to monitor and control remote access sessions (VPN, RDP, etc.).
- Ensure remote access is authorized, logged, and actively monitored for anomalies or misuse.
- Apply technical controls to enforce policy-based restrictions (e.g., time-of-day, device compliance, MFA).

This is an existing requirement and marked Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

- SIEM dashboards or alerts showing real-time monitoring of remote sessions.
- VPN/RDP gateway logs integrated with automated alerting for suspicious activity.
- Conditional Access or NAC (Network Access Control) policies enforcing compliance checks.
- Documentation of automated controls (e.g., session termination on policy violation).

○ Yes
○ No

3. (2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION
[Existing] [Priority 1]

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

Please provide the auditor a copy of FIPS 140-2 or higher.

CJIS Requirement:

CJIS Security Policy § 5.10.1.2 and 5.5 (Access Control) requires that remote access sessions (VPN, RDP, etc.) use FIPS 140-2 or higher validated cryptographic modules to protect the confidentiality and integrity of transmitted CJI. This applies to all remote access methods, including administrative sessions.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

• VPN and remote access configuration screenshots showing TLS 1.2+ or IPsec with FIPS-validated modules.
• Vendor documentation or system settings confirming FIPS mode enabled.
• A copy of the FIPS 140-2 or FIPS 140-3 certificate for the cryptographic module used (e.g., from NIST CMVP listing).
• Policy stating encryption requirements for remote access.

☐ I have read and will comply.

8. AC-18 WIRELESS ACCESS[Existing] [Priority 2]

Does the agency establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access, and authorize each type of wireless access to the system prior to allowing such connections?

CJIS Requirement:

CJIS Security Policy § 5.10.4.3 requires agencies to define and enforce configuration and connection requirements for all wireless access points and devices. Agencies must implement guidance for secure wireless connectivity and ensure that each type of wireless access is formally authorized before being enabled.

Status: Existing requirement, Priority 2 in the CJIS Requirements Companion.

Evidence Examples:

- **Policy or SOP defining:**
- **Approved wireless technologies and configurations.**
- **Encryption standards (e.g., WPA2/WPA3).**
- **Authentication requirements for wireless connections.**
- **Roles responsible for authorizing wireless access.**
- **Wireless Access Authorization Records:**
- **Documentation showing AO or designated official approval for each wireless access type.**

- **Change management tickets for enabling wireless connectivity.**
- **Configuration Settings:**
- **Screenshots or exported configs showing SSID, encryption, and access control settings.**
- **Network segmentation details for wireless traffic.**
- **Access Control Logs:**
- **Logs showing authorized devices connecting to wireless networks.**
- **Evidence of monitoring for unauthorized wireless access attempts.**
- **System Security Plan (SSP):**
- **Sections describing wireless access controls and authorization processes.**

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. 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?

CJIS Requirement:

CJIS Security Policy § 5.13 Wireless Access Control requires that:

• Wireless access to systems handling CJI must be secured with strong authentication (authorized users and agency-controlled devices).
• Wireless communications must be encrypted using FIPS 140-2 or higher validated cryptographic modules to protect confidentiality and integrity.
• Agencies must implement controls to prevent unauthorized wireless connections and rogue devices.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

• Wireless Access Policy specifying authentication and encryption requirements.
• Configuration screenshots showing WPA2-Enterprise or WPA3 with 802.1X authentication tied to agency identity provider.
• Documentation or vendor certificate showing FIPS 140-2/140-3 validation for wireless encryption modules.
• MDM or NAC reports showing only authorized devices can connect.

○ Yes
○ No
○ N/A

2. AC-18(3) WIRELESS ACCESS | DISBALE WIRELESS NETWORKING
[Existing] [Priority 2]

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

CJIS Requirement:

CJIS Security Policy § 5.10.4.3 requires agencies to ensure that wireless networking features on system components are disabled when not needed, prior to deployment, to prevent unauthorized wireless connections and reduce attack surface.

Status: Existing requirement, Priority 2 in the CJIS Requirements Companion.

Evidence Examples:

• Policy or SOP defining:
• Conditions under which wireless networking must be disabled.
• Roles responsible for verifying wireless disablement prior to deployment.
• Configuration Records:
• Screenshots or exported settings showing wireless interfaces disabled.
• Device hardening checklists confirming wireless disablement.
• Deployment Documentation:
• Pre issuance validation logs or sign off forms confirming compliance.
• Change management tickets for disabling wireless features.
• System Security Plan (SSP):
• Sections describing wireless disablement requirements and verification process.

○ Yes
○ No

3. Please provide:

1. The methods used to authenticate authorized users and agency-controlled devices for wireless access (e.g., WPA2-Enterprise, 802.1X, certificate-based authentication).
2. The encryption protocols in use (e.g., AES-CCMP, WPA3) and confirmation that they are FIPS 140-2 or 140-3 validated.
3. Documentation or screenshots showing wireless security configurations and enforcement of these controls.
4. Any policy or procedure governing wireless access to systems that process CJI.

☐ I have read and will comply.

9. AC-19 ACCESS CONTROL FOR MOBILE DEVICES
[Existing] [Priority 1]

Has the agency:
a. Established and documented configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, including when such devices operate outside controlled areas;
b. Authorized and documented the process for connecting mobile devices to organizational systems; and
c. Implemented mechanisms to enforce these requirements and monitor compliance?

CJIS Requirement:

CJIS Security Policy § 5.13 Mobile Device Management requires agencies to:

- **Define and document configuration and connection requirements for mobile devices that access or store CJI.**
- **Ensure mobile devices are agency-controlled and authorized before connecting to organizational systems.**
- **Implement technical mechanisms (e.g., MDM, NAC) to enforce compliance and monitor device posture.**
- **Apply these controls even when devices operate outside controlled areas.**

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

• Mobile Device Policy specifying configuration standards (encryption, screen lock, inactivity timeout, remote wipe).
• Authorization workflow for mobile device enrollment (forms, MDM enrollment logs).
• MDM console screenshots showing compliance enforcement and monitoring.
• Reports showing device compliance checks and remediation actions.

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. AC-19(5) ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE OR CONTAINER-BASED ENCRYPTION
[Existing] [Priority 2] - [DPS Enhanced Priority 1]

Does the agency:

• Employ full-device or container-based encryption to protect the confidentiality and integrity of information on mobile devices (full- and limited-feature operating systems) authorized to process, store, or transmit CJI; and

• Ensure encryption is enforced and verified through technical controls (e.g., MDM compliance policies)?

Please provide evidence (e.g., configuration reports, screenshots, or policy documentation) confirming that all areas where CJI may be stored on mobile devices are encrypted.

○ Yes
○ No

10. AC-20 USE OF EXTERNAL SYSTEMS
[Existing] [Priority 1]

Has the agency:

• Defined and documented conditions under which external systems (including BYOD, contractor systems, or cloud services) may be used to access organizational resources;

• Established and enforced security requirements for external systems (e.g., encryption, authentication, compliance with agency policies); and

• Implemented an authorization process for approving the use of external systems?

CJIS Requirement:

CJIS Security Policy § 5.5 Access Control requires agencies to:
• Define conditions for using external systems (BYOD, contractor-owned devices, or cloud services) to access CJI or organizational resources.
• Enforce security requirements for those systems, including encryption, authentication, and compliance with agency policies.
• Implement a formal authorization process before granting access from external systems.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

- Policy specifying conditions for external system use (BYOD, contractor systems, cloud).
- Security requirements documentation (FIPS encryption, MFA, device hardening).
- Authorization workflow records for approving external system access.
- Vendor agreements or CJIS Security Addendum for cloud services.

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. How does the agency authorize individuals to use external systems (e.g., personal laptops, third-party devices, non-agency networks) to access CJIS systems or Criminal Justice Information (CJI)?

What security measures and monitoring processes are in place to ensure this access is compliant and protected?

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

1. IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) [Existing][Priority 1]

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?

CJIS Requirement:

CJIS Security Policy § 5.6 Identification and Authentication requires that:

- Every organizational user accessing CJI systems must have a unique identifier (no shared or generic accounts).
- Authentication must be performed before granting access, and the system must associate all actions with the authenticated user for accountability.
- Applies to all access methods (local, remote, application-level).

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

- Active Directory or identity provider (IdP) user list showing named accounts only.
- Policy prohibiting shared or generic accounts.
- Authentication logs mapping user IDs to system actions.
- Screenshots of MFA enforcement for organizational accounts.

○ Yes
○ No

2. IA-2(1) (2) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS & NON-PRIVILEGED ACCOUNTS

Please describe how the agency implements multi-factor authentication (MFA) for:

• Privileged accounts (e.g., system administrators, elevated roles); and
• Non-privileged accounts (e.g., standard user accounts).

Include details on:

• MFA technologies used (e.g., smart cards, OTP, authenticator apps, biometrics).
• Enforcement mechanisms (e.g., conditional access, identity provider settings).
• Any exceptions or compensating controls.

CJIS Requirement:

CJIS Security Policy § 5.6 Identification and Authentication require:

• Privileged Accounts: MFA is mandatory for all remote access and for privileged accounts accessing CJI systems
• Non-Privileged Accounts: MFA is required for remote access to CJI systems and strongly recommended for all interactive sessions.

• MFA must combine two or more factors:
• Something you know (password/PIN)
• Something you have (smart card, OTP token, authenticator app)
• Something you are (biometric)

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

• Screenshots of MFA enforcement in identity provider (e.g., Azure AD Conditional Access, Okta policies).
• VPN/RDP gateway configuration showing MFA challenge.
• MFA enrollment reports for privileged and non-privileged accounts.
• Policy requiring MFA for remote access and privileged accounts.

3. IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION
[Existing] [Priority 2]

Does the agency uniquely identify and authenticate agency-managed devices before establishing network connections, and ensure that locally connected devices are approved, identified, and authenticated prior to accessing agency assets?

CJIS Requirement:

CJIS Security Policy § 5.10.4.4 requires agencies to implement controls that uniquely identify and authenticate all agency-managed devices before allowing them to connect to the network. For local connections, devices must be explicitly approved and authenticated prior to accessing any agency system or resource.

Status: Existing requirement, Priority 2 in the CJIS Requirements Companion.

Evidence Examples:

• Policy or SOP defining:
• Device identification and authentication requirements.
• Approval process for locally connected devices.
• Roles responsible for device authorization.
• Configuration Records:
• Device inventory with unique identifiers (MAC address, certificates).
• Network access control (NAC) or endpoint management settings enforcing device authentication.
• Authorization Logs:
• Records showing device approval prior to connection.
• Logs from NAC or MDM systems confirming device authentication events.
• System Security Plan (SSP):
• Sections describing device identification and authentication processes.

○ Yes
○ No

4. IA-4 IDENTIFIER MANAGEMENT
[Priority 1]

Does the agency:

- Uniquely identify each user and device that requires access to Criminal Justice Information (CJI);
- Implement controls to prevent identifier reuse or sharing among users; and
- Maintain processes for issuing, managing, and retiring identifiers in accordance with CJIS and NIST IA-4 requirements?

CJIS Requirement:

CJIS Security Policy § 5.6 Identification and Authentication requires agencies to:

- Assign unique identifiers to every user and device accessing CJI systems.
- Prevent reuse or sharing of identifiers to maintain accountability.
- Establish documented processes for issuing, managing, and retiring identifiers, aligned with CJIS and NIST IA-4 standards.
- Ensure identifiers are linked to individual accountability for all system actions.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

- Identity and Access Management (IAM) policy detailing identifier lifecycle (creation, modification, retirement).
- Active Directory or IdP configuration showing unique usernames and device IDs.
- Logs demonstrating no shared or generic accounts.
- Procedures for retiring identifiers when personnel separate or devices are decommissioned.

○ Yes
○ No

5. IA-5 – AUTHENTICATOR MANAGEMENT
[Priority 1]

Does the agency implement and enforce controls for the lifecycle management of authenticators (e.g., passwords, passphrases, tokens, or biometrics) used to access systems that process, store, or transmit Criminal Justice Information (CJI)?

If remote access to CJI exists:

• Does the agency implement Advanced Authentication (MFA) in accordance with CJIS Security Policy §5.6.2.2?

Please provide evidence of policy, technical enforcement (e.g., system configuration), and monitoring processes.

CJIS Requirements:

CJIS Security Policy §5.6 (Identification and Authentication) requires agencies to implement controls for the secure management of authenticators used to access systems that process, store, or transmit Criminal Justice Information (CJI). Agencies must:

- Manage the full lifecycle of authenticators, including creation, issuance, distribution, storage, use, and revocation.
- Ensure authenticators are uniquely assigned to individual users and prohibit shared credentials.
- Require the use of secure authenticators (e.g., passwords, passphrases, tokens, biometrics) appropriate to the level of access and risk.
- Protect authenticators in storage and transmission (e.g., hashing, encryption, no plaintext storage).
- Ensure default or vendor-supplied credentials are changed prior to system use.
- Implement controls to prevent the use of weak or compromised authenticators.
- Require authenticators to be changed when compromised or suspected of compromise.
- Enforce password reuse restrictions (password history or similar controls).
- Ensure accounts and associated authenticators are disabled or revoked promptly when access is no longer required (e.g., termination, role change).

Remote Access Requirement:

- In accordance with CJIS Security Policy §5.6.2.2, agencies shall implement Advanced Authentication (Multi-Factor Authentication) for all remote access to CJI.

Evidence Examples:

Agencies should be prepared to provide documentation and/or demonstrations showing both policy and technical enforcement, including:

Policy & Procedure Documentation

- Agency authentication or password policy
- Account management procedures (provisioning, modification, deactivation)
- Remote access / MFA policy
- Incident response procedures addressing compromised credentials

Technical Configuration Evidence

- Active Directory / system password policy settings (e.g., length, history, lockout)
- Screenshots or exports showing:
- Password requirements
- Account lockout thresholds
- Password history enforcement
- MFA configuration for:
- VPN access
- Remote desktop / CJIS system access
- System settings showing disabled default accounts or renamed administrative accounts

Account Management Evidence

- Sample user account listings showing:
- Unique user IDs
- Disabled accounts for terminated users
- Onboarding/offboarding records demonstrating:
- Account creation approval
- Timely account deactivation

Security & Protection Evidence

- Documentation or screenshots showing:
- Passwords are not stored in plaintext
- Use of hashing/encryption mechanisms
- Vendor/system documentation confirming secure authenticator storage (if applicable)

Monitoring & Compliance Evidence

- Logs or reports showing:
- Failed login attempts / lockouts
- Authentication-related alerts
- Evidence of periodic account reviews or audits

○ Yes
○ No

Primary question answered Yes

1. IA-5 (1) AUTHENTICATOR MANAGEMENT | AUTHENTICATOR TYPES
[Priority 1]

Which authenticator types does the agency currently use for user authentication?

(Select all that apply and provide supporting evidence such as policy documents, system configurations, or screenshots.)

☐ (a) Memorized Secret Authenticators and Verifiers (e.g., passwords)
☐ (b) Look-Up Secret Authenticators and Verifiers (e.g., recovery codes)
☐ (c) Out-of-Band Authenticators and Verifiers (e.g., SMS or voice call verification)
☐ (d) OTP Authenticators and Verifiers (e.g., time-based one-time passwords via apps or tokens)
☐ (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 [Existing] [Priority 1]

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

CJIS Requirement:

CJIS Security Policy § 5.6 Identification and Authentication requires that when agencies implement public key-based authentication, they must:

• Use FIPS 140-2 or higher validated cryptographic modules for key generation, storage, and operations.
• Ensure PKI certificates are issued by a trusted Certificate Authority (CA) and managed according to CJIS and NIST guidelines.
• Apply PKI for authentication of users, devices, or systems accessing CJI, especially for remote or privileged access scenarios.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

• PKI implementation documentation (architecture diagrams, CA hierarchy).
• Certificate policy and procedures (issuance, renewal, revocation).
• Screenshots or logs showing PKI-based authentication in use (e.g., smart card login, TLS mutual authentication).
• FIPS 140-2/140-3 certificate for cryptographic modules used in PKI operations.

○ 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?

CJIS Requirement:

CJIS Security Policy § 5.6 Identification and Authentication requires agencies that use public key-based authentication or PKI to:

• Protect private keys: Ensure only authorized users/processes can access the private key associated with their identity.
• Identity Mapping: Map the authenticated certificate identity to the correct user account for accountability.
• Certificate Validation: Validate certificates by building a certification path to a trusted root CA and checking revocation status (CRL or OCSP).
• Revocation Data Cache: Maintain a local cache of revocation data to allow validation even if the CA or OCSP responder is temporarily unavailable.
• Use FIPS 140-2 or higher validated cryptographic modules for all PKI operations.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

• PKI architecture documentation showing trust anchors and certificate validation process.
• System configuration enforcing certificate validation and revocation checks (CRL/OCSP).
• Logs showing successful certificate path validation and revocation status checks.
• Documentation of local CRL cache implementation and refresh schedule.
• Access control policy for private key storage (e.g., smart card PIN, HSM access logs).

○ Yes
○ No

2. If yes, please describe:

• The scope of PKI usage (e.g., privileged accounts, VPN, email encryption, device certificates).
• How keys and certificates are issued, managed, and revoked.
• Technical enforcement and monitoring processes.

Provide supporting evidence such as PKI policy, certificate authority configuration, and sample certificate details.

Section - Policy Area 7 - Configuration Management (CM)

1. CM-2 BASELINE CONFIGURATION
[Existing] [Priority 1]

Does the agency maintain current documentation of system baseline configurations, including a network diagram or equivalent documentation, that identifies systems and network components involved in the processing, storage, or transmission of Criminal Justice Information (CJI)?

The network diagram should identify, as applicable:

- **Firewalls, routers, and switches**
- **Wireless access points and controllers**
- **All servers (application, database, domain controllers)**
- **Workstations, laptops, and mobile data terminals (MDTs)**
- **LiveScan devices and fingerprint transmission paths**
- **Backup servers, storage appliances, and off-site/cloud backup locations**

- VPN connections and remote access paths
- CJIS and non-CJIS system boundaries
- VLAN segmentation
- Security appliances (IDS/IPS, proxies, content filters)
- DMZs or isolated networks
- Interfaces with third-party systems or vendors
- Cloud services or hosted solutions (if applicable)
- CJIS Security Zones and trust boundaries
- Network connections to criminal justice information systems (NCIC, state CJIS)

Please provide:

- The current network diagram or documentation which should be kept current and updated following significant system or network changes.
- Documentation of the process for maintaining and reviewing the diagram.
- Evidence of change management for updates.

○ Yes
○ No

Primary question answered Yes

1. CM-2(7) BASELINE CONFIGURATION | CONFIGURE SYSTEMS AND COMPONENTS FOR HIGH-RISK AREAS[Existing] [Priority 1]

Does the agency issue devices with CJIS-compliant configurations to individuals traveling to locations identified as high-risk, and upon their return, examine the devices for signs of tampering, purge and reimage drives or devices as required, and verify that all security controls are restored and fully functional?

CJIS Requirement:

Agencies must apply enhanced configuration controls for devices used in high risk environments, including pre deployment hardened baselines and post travel procedures to validate device integrity, remove potential compromise (e.g., purge/reimage), and confirm that all required CJIS controls are in place and operating as intended.

Status: Existing requirement, Priority 1.

Evidence Examples:

- Policy or SOP defining:
- Criteria for “high risk” locations (e.g., foreign travel, hostile networks, public hotspots).
- Required CJIS compliant baseline configurations for travel devices (encryption, MFA, allowlisting, VPN, logging).
- Post travel procedures: tamper inspection, purge/reimage, control verification, and incident referral criteria.

- Travel Device Issuance Records:
- Approval for issuing hardened devices for high risk travel.
- Baseline configuration checklists signed off prior to deployment.

- Post Travel Review Records:
- Tamper inspection logs (physical integrity checks).
- Evidence of purge/reimage actions (tickets, scripts, imaging logs).
- Verification that all required security controls are restored and functional (control validation checklist).

- System Security Plan (SSP):
- Sections describing high risk travel configurations and post travel remediation/validation workflows.

- Change Management & Monitoring:
- Tickets documenting temporary configuration changes for travel and subsequent rollback.
- Monitoring dashboards/reports showing device posture before and after travel.

○ Yes
○ No

2. CM-3 CONFIGURATION CHANGE CONTROL
[Priority 2]

Does the agency have a documented configuration change control process that identifies which system changes require control, evaluates and approves proposed changes with security and privacy impact considerations, documents and implements approved changes, retains change records for at least two years, monitors change-related activities, and oversees the process through designated configuration management personnel or a formal review board?

CJIS Requirement:

The agency must maintain a documented configuration change control process that identifies which system changes require configuration control, ensures proposed changes are evaluated with documented security and privacy impact analyses, approves or disapproves changes prior to implementation, documents and implements approved changes, retains configuration controlled change records for at least two years, monitors configuration change activities, and oversees the process through designated configuration management personnel or a formal Configuration Control Board (CCB) or Change Advisory Board (CAB).

Status: Existing requirement, Priority 2.

Evidence Examples:

Policy or SOP defining:
• Types of system changes that require configuration control.
• Procedures for submitting, reviewing, and approving changes.
• Requirements for conducting security and privacy impact analyses before approval.
• Documentation requirements for change decisions and two year record retention.
• Monitoring procedures for verifying changes are implemented as approved.
• Roles and responsibilities for configuration management personnel, CCB, or CAB oversight.

Configuration Change Requests (Forms, Tickets, or Digital Records):
• Submitted change requests describing proposed changes and justification.
• Documented security and privacy impact analyses attached to each request.
• Approval or disapproval records showing authorized reviewers' decisions.
• Evidence that only approved changes were implemented (deployment logs, ticket closures).

Configuration Change Logs and Records:
• Logs showing all configuration controlled changes with dates, identifiers, and version updates.
• Records retained for at least two years demonstrating historical change activity.
• Documentation of rollback procedures if changes were reversed.

Change Oversight Records:
• Minutes or logs of Configuration Control Board or Change Advisory Board meetings.
• Attendance records showing designated configuration management personnel participated.
• Evidence of periodic monitoring or audits of change activities.

System Security Plan (SSP):
• Sections describing the configuration change control workflow.
• Defined roles and responsibilities for change submission, review, approval, implementation, and monitoring.

○ Yes
○ No

3. CM-5 ACCESS RESTRICTIONS FOR CHANGE
[Existing] [Priority 1]

Does the agency define, document, approve, and enforce physical and logical access restrictions for changes to system components, configurations, and software?

CJIS Requirement:

CJIS Security Policy § 5.10.4.1 requires agencies to implement access restrictions for changes to system components. This includes defining roles authorized to make changes, documenting approval processes, and enforcing both physical and logical controls to prevent unauthorized modifications.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

- Policy or SOP defining:
- Which components/configurations/software require restricted access.
- Roles authorized to make changes.
- Approval workflow and emergency change procedures.
- Access control configurations:
- Role-based access control (RBAC) settings.
- Privileged account management.
- MFA for administrative accounts.
- Physical access logs for server rooms or network closets.
- Change management records:
- Tickets showing request, approval, and implementation.
- System audit logs showing configuration changes and administrative actions.

○ Yes
○ No

Primary question answered Yes

1. Please confirm and provide evidence for the following:

1. Has the agency defined and documented roles authorized to perform configuration changes?
2. Are logical access controls (e.g., RBAC, privileged access management) implemented to ensure that only authorized personnel can perform or approve changes?
3. Are physical access controls in place for systems where configuration changes can occur?
4. Does the agency approve and record changes to ensure accountability and traceability?

○ Yes
○ No

2. Please provide:

• Access control lists (ACLs) or role-based permissions showing who is authorized to make changes.
• Policy and procedures related to access restrictions for configuration changes.
• Evidence of recent changes demonstrating:
• Approval by designated personnel.
• Enforcement of access restrictions (e.g., logs showing only authorized accounts executed changes).

☐ I have read and will comply.

4. CM-6 CONFIGURATION SETTINGS
[Priority 1]

Has the agency:
a. Established and documented configuration settings for system components that reflect the most restrictive mode consistent with operational requirements, using best practices such as DISA STIGs, CIS Benchmarks, or FIPS standards?
b. Implemented these configuration settings across applicable components?
c. Identified, documented, and approved any deviations from established configuration settings for components that store, process, or transmit CJI based on operational needs?
d. Monitored and controlled changes to configuration settings in accordance with organizational policies and procedures?

Please provide:
- Configuration baseline documentation.
- Records of approved deviations.
- Evidence of implementation (e.g., screenshots, system hardening reports).
- Monitoring logs or reports showing configuration compliance.

CJIS Requirement:

CJIS Security Policy § 5.10.4.2 requires agencies to establish, document, and enforce configuration settings for information systems that process, store, or transmit CJI. These settings must be based on industry-recognized hardening standards (e.g., DISA STIGs, CIS Benchmarks) and must be monitored for compliance. Deviations must be documented and approved.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

- Configuration baseline documentation:
- Hardening guides or baseline checklists aligned with DISA STIGs, CIS Benchmarks, or FIPS standards.
- Records of approved deviations:
- Change management tickets or waiver forms showing justification and approval.
- Evidence of implementation:
- Screenshots of system settings (e.g., password policies, audit logging enabled).
- System hardening reports from tools like CIS-CAT, Nessus, or SCAP.
- Monitoring logs or reports:
- Compliance scans or dashboards showing adherence to baseline configurations.
- Alerts for unauthorized configuration changes.

○ Yes
○ No
○ N/A

5. CM-7 (1)(2)(5) LEAST FUNCTIONALITY
[Existing] [Priority 1]

Does the agency ensure that systems storing, processing, or transmitting CJI are configured to provide only essential capabilities required for operations by:
- Prohibiting or restricting unnecessary functions, ports, protocols, software, and services;
- Conducting periodic reviews (at least annually or upon system changes/incidents) to identify and remove or disable nonessential or insecure components;
- Preventing the execution of unauthorized programs in accordance with defined rules of behavior or usage policies; and
- Implementing a deny-all, permit-by-exception policy for software execution, including maintaining and annually updating a list of authorized software?

Please provide:

- System hardening standards or configuration baselines.
- Authorized software list and date of last update.
- Evidence of periodic reviews and remediation actions.
- Technical enforcement details (e.g., application whitelisting, GPO settings, endpoint protection configurations).

CJIS Requirement:

CJIS Security Policy § 5.10.4.3 (Configuration Management) requires agencies to enforce least functionality, ensuring systems provide only essential capabilities necessary for operations. Controls must include the prohibition/restriction of unnecessary services, ports, protocols, and software; periodic reviews to identify/remove nonessential components; and deny-by-default, allow-by-exception rules for software execution (e.g., application whitelisting). This aligns with NIST SP 800-53 CM-7 and enhancements (1) least functionality enforcement, (2) nonessential capabilities review/removal, and (5) deny-all, permit-by-exception execution policies for systems handling CJI.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

- System hardening standards or configuration baselines
- Baselines aligned to DISA STIGs, CIS Benchmarks, or agency hardening guides that explicitly disable nonessential services (e.g., SMBv1, Telnet, FTP), lock down ports/protocols, and remove unused software.
- Authorized software list and date of last update
- A centrally maintained, versioned allowlist of approved applications (by name, version, publisher/hash), reviewed at least annually.
- Evidence of periodic reviews and remediation actions
- Annual or change-driven review reports, with findings and remediation (e.g., removal of unused services, deinstallation of unauthorized tools, port closures).
- Technical enforcement details
- Application control: Windows Defender Application Control (WDAC) / AppLocker rules, macOS Application Control/PPPC profiles, Linux SELinux/AppArmor profiles.
- Endpoint protection configurations showing deny-by-default application execution, script controls, and blocking of unsigned binaries.
- GPO screenshots demonstrating enforcement (e.g., SRP/AppLocker policies, PowerShell Constrained Language Mode, script execution policies).
- Network controls showing disabled/blocked ports and legacy protocols (e.g., via firewall policies).

○ Yes
○ No

6. CM-8, (1),(3) System Component Inventory
[Priority 1]

Does the agency:

1. Develop, document, and maintain an inventory of all system components (hardware, software, virtual, and firmware) within the system boundary that:

• Accurately reflects the current system state;
• Includes all components without duplication or misassignment;
• Is maintained at a level of granularity necessary for effective tracking and reporting;
• Includes, at a minimum: installation date, model, serial number, manufacturer, supplier, component type, software owner, software version, license information, and physical location;
• Is reviewed and updated at least annually and whenever components are added, removed, or updated?

2. Use automated mechanisms, either continuously or at least weekly, to detect unauthorized hardware, software, and firmware components; and upon detection:

• Disable or isolate the unauthorized components; and
• Notify organizational personnel with security responsibilities?

CJIS Requirement:

CJIS Security Policy § 5.10 – Configuration Management (Inventory of system components aligned to NIST SP 800-53 CM 8 and enhancements (1) and (3)) requires agencies to maintain a comprehensive, accurate inventory of all components that store, process, or transmit CJI, and to employ automated discovery and alerting to identify and respond to unauthorized components. Inventories must be reviewed/updated at least annually and upon any change, and agencies must promptly isolate/disable unauthorized assets and notify designated security personnel.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

• System Component Inventory / CMDB (current export or report):
• Hardware: asset tag, device name, model, serial number, manufacturer, supplier, component type (server/workstation/network), installation date, warranty status, physical location, owner/ custodian.
• Software: application name, version, publisher, deployment date, license details, owner, device association, installation count, approval status.
• Virtual/Cloud: VM name, host, vCenter/Hypervisor, subscription/tenant, region, image/AMI ID, security zone.
• Firmware & BIOS versions (including network/IoT/MDT devices, printers, LiveScan).
• Automated discovery & detection configurations:
• Screenshots/reports from Intune/Endpoint Manager, SCCM/MECM, Jamf, Lansweeper, Tenable/Nessus, Rapid7, CrowdStrike, or Active Directory showing asset discovery and weekly (or continuous) scans.
• NAC (e.g., Cisco ISE/Aruba ClearPass) policies for rogue device detection and quarantine/ VLAN isolation.
• SIEM/EDR rules & alert samples for unauthorized software/firmware.
• Response evidence for unauthorized components:
Tickets/logs showing detection isolation/quarantine notification to SOC/IS team remediation.
• Network block lists, MDM retire/wipe actions, EDR containment records.
• Review/Update documentation:
• Annual inventory review sign-off, reconciliation procedures, and delta reports after major deployments/retirements.
• Reconciliations with procurement/receiving records and disposal certificates (to prevent ghost assets/duplication).

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. Please provide:

• Current system inventory report (including hardware, software, virtual, and firmware components) and the date of last update.
• Inventory management policy and procedures that outline how the inventory is maintained and reviewed.
• Evidence of automated detection and response for unauthorized components, such as:
• Logs or alerts from asset management or SIEM tools.
• Documentation of actions taken to disable or isolate unauthorized components.

☐ I have read and will comply.

7. CM-10 SOFTWARE USAGE RESTRICTIONS
[Priority 3]

Does the agency have a documented process ensuring that software and associated documentation are used in accordance with contract agreements and copyright laws, that the use of licensed software is tracked to control copying and distribution, and that peer-to-peer file-sharing capabilities are controlled and documented to prevent unauthorized distribution or reproduction of copyrighted material?

CJIS Requirements:

The agency must ensure that all software and associated documentation are used in compliance with contractual agreements and copyright laws, maintain processes to track and control the use of software governed by quantity-based licenses to prevent unauthorized copying or distribution, and implement controls to monitor, restrict, and document the use of peer-to-peer (P2P) file-sharing technologies to ensure they are not used for the unauthorized distribution, display, performance, or reproduction of copyrighted materials.

Evidence Examples:

Policy or SOP defining:
• Requirements for using software and associated documentation in accordance with contract agreements and copyright laws.
• Procedures for tracking software installations governed by quantity based licensing to prevent unauthorized copying or distribution.
• Controls restricting and monitoring the use of peer to peer (P2P) file sharing technologies to prevent unauthorized distribution, display, performance, or reproduction of copyrighted materials.
• Processes for approving software requests and verifying license compliance before installation.

Software Inventory and License Management Records:
• Comprehensive software inventory showing installed applications and associated license counts.
• Proof of license entitlements matching installed software quantities.
• Reports from software asset management tools demonstrating license compliance and removal of unapproved software.
• Documentation of license keys, purchase records, and renewal tracking.

Peer to Peer Usage Controls:
• Network or endpoint protection logs showing P2P traffic is blocked, restricted, or monitored.
• Firewall rules or endpoint configuration settings showing P2P applications are disabled or prohibited.
• Exception documentation for any approved P2P tools, including justification and monitoring requirements.

System Configuration and Endpoint Management Evidence:
• Application allowlisting or blocklisting configurations preventing unauthorized software installation.
• Screenshots or exports from endpoint management tools showing approved software lists.
• Group Policy Objects (GPOs) or device configuration profiles enforcing software restrictions.

Training and Awareness Records:
• User training materials covering software licensing, copyright compliance, and P2P restrictions.
• Employee acknowledgment forms confirming understanding of software usage policies.

System Security Plan (SSP):
• Sections describing software usage restriction controls, software license tracking processes, and peer to peer monitoring or blocking measures.

○ Yes
○ No

8. CM-11 USER-INSTALLED SOFTWARE
[Priority 2]

Does the agency have a documented policy that governs user installation of software, enforce these software installation restrictions through automated technical controls, and monitor compliance with these policies through automated methods at least weekly?

CJIS Requirement:

The agency must establish and enforce policies that govern user-installed software, apply automated controls to restrict unauthorized software installations, and monitor compliance with these installation policies through automated methods at least weekly.

Evidence Examples:

Policy or SOP defining:
• Agency-level policies authorizing or prohibiting user installation of software, including exceptions only with explicit privileged status.
• Requirements for using automated technical controls (e.g., privileged access restrictions,

endpoint protection mechanisms) to enforce installation policies.
• Procedures for automated monitoring of installation compliance, performed at least weekly, and escalation processes for violations.

Technical Enforcement Controls:
• Endpoint or configuration management screenshots showing restrictions on software installation by standard users.
• Firewall, application manager, or endpoint protection logs demonstrating blocked installation attempts.

Monitoring Records:
• Automated weekly compliance reports showing permitted vs. unauthorized software installations.
• Logs/events capturing alerts or notifications when unauthorized software installations occur.

Configuration and System Documentation:
• Group Policy Objects (GPOs), configuration settings, or device profiles enforcing software installation restrictions.
• System architecture or design records specifying enforcement and monitoring mechanisms.

System Security Plan (SSP):
• Sections detailing the user-installed software policy, technical enforcement controls, and weekly automated monitoring workflows.

○ Yes
○ No

Section - Policy Area 8 - Media Protection (MP)

1. MP-1 POLICY AND PROCEDURES
[Existing] [Priority 1]

Does the agency have a formal media protection policy that:

- Defines roles and responsibilities for handling CJI on digital and non-digital media;
- Outlines procedures for secure storage, transport, and disposal of media; and
- Is reviewed and updated at least annually or as required by CJIS Security Policy?

CJIS Requirement:

CJIS Security Policy § 5.8 – Media Protection requires agencies to establish and maintain a formal policy and documented procedures for protecting media containing CJI. This includes defining roles and responsibilities, specifying secure handling methods for digital and non-digital media, and ensuring proper storage, transport, and disposal. The policy must be reviewed and updated annually or when significant changes occur.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

- Media Protection Policy Document:
- Defines roles (e.g., IT staff, evidence custodians, disposal vendors).

• Covers secure storage (locked cabinets, encrypted drives), transport (chain-of-custody forms, tamper-evident packaging), and disposal (degaussing, shredding, certified destruction).
• Specifies review/update frequency (at least annually).
• Procedures or SOPs:
• Detailed steps for handling CJI on USB drives, CDs/DVDs, backup tapes, printed reports.
• Chain-of-custody documentation templates.
• Annual Review Records:
• Sign-off sheets or version history showing last review date.
• Training Records:
• Evidence that staff handling media completed training on policy and procedures.
• Vendor Certifications (if using third-party disposal):
• Certificates of destruction and compliance with CJIS requirements.

○ Yes
○ No

Primary question answered Yes

1. How does the agency validate that all authorized individuals who handle CJI have acknowledged the media protection policy and related procedures (e.g., signed acknowledgment forms, LMS attestations, onboarding records)?

2. Please provide:

• A copy of the current Media Protection Policy and any related step-by-step procedures that address handling of CJI on digital and non-digital media.
• Documentation showing the date of last review or update of the policy to confirm it is current.
• Evidence of staff awareness or training on media handling requirements (e.g., training records, sign-in sheets, or LMS reports).

☐ I have read and will comply.

2. MP-4 MEDIA STORAGE
[Existing] [Priority 1]

Does the agency:

1. Physically control and securely store digital and non-digital media within physically secure locations or controlled areas?
2. Encrypt CJI on digital media when physical and personnel restrictions are not feasible?
3. Protect digital and non-digital media until the media is destroyed or sanitized using approved equipment, techniques, and procedures?

CJIS Requirement:

CJIS Security Policy § 5.8.2 – Media Storage requires agencies to ensure that all media

containing CJI is physically secured in controlled areas or locked containers when not in use. If physical and personnel controls cannot be guaranteed (e.g., offsite storage, transport), CJI must be encrypted using FIPS 140-2 or higher validated cryptographic modules. Media must remain protected until it is sanitized or destroyed using CJIS-approved methods.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

- Media Storage Policy/SOP:
- Defines secure storage locations (server rooms, evidence lockers, locked cabinets).
- Specifies encryption requirements for portable media (USB drives, backup tapes).
- Physical Security Evidence:
- Photos or diagrams of secure storage areas (locked cabinets, badge-controlled rooms).
- Access logs for media storage areas.
- Encryption Evidence:
- Screenshots showing FIPS mode enabled on backup systems or removable media encryption (BitLocker, VeraCrypt with FIPS module).
- Vendor documentation confirming FIPS 140-2 compliance.
- Protection Until Disposal:
- Chain-of-custody logs for media in storage.
- Certificates of destruction or sanitization reports.
- Approved sanitization methods (degaussing, shredding, wiping tools with NIST/CJIS compliance).

○ Yes
○ No
○ n/a

3. MP-5 MEDIA TRANSPORT
[Existing] [Priority 1]

Describe the agency's process for protecting CJI when physically transporting digital or physical media (e.g., USB drives, CDs, laptops, printed documents). Include details on encryption, chain-of-custody, and authorized personnel handling.

CJIS Requirement:

CJIS Security Policy § 5.8.3 – Media Transport requires agencies to protect CJI during transport of both digital and non-digital media. Agencies must:
• Ensure authorized personnel handle and accompany CJI media;
• Use encryption (FIPS 140-2 or higher validated cryptographic modules) for digital media when physical controls cannot be guaranteed;
• Maintain chain-of-custody documentation; and
• Apply procedures that prevent unauthorized access, disclosure, modification, or loss during transport.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Process Description (What the Auditor Should See)

1. Pre-Transport Authorization & Preparation

• Approval: Transport must be approved by the data owner or IS/security officer; purpose and destination documented.
• Packaging:
• Digital media (USB, SSDs, tapes, laptops): Stored in tamper-evident bags; device encrypted

(BitLocker, hardware crypto, or backup media encryption) with FIPS 140-2/140-3 validated modules; verify encryption is enabled before departure.
• Physical media (printed reports): Placed in sealed, labeled, tamper-evident envelopes/ containers marked with sensitivity (no CJI on external labels).
• Access Minimization: Only authorized, trained personnel may handle/transport CJI media.

2. Chain-of-Custody

• Log entries include: media ID, description, sensitivity, source, destination, date/time, handler name, purpose, seal/bag ID, encryption confirmation, and expected arrival.
• Transfers: Each custody transfer requires signature (or verified electronic sign-off) with date/ time; seals are inspected and logged.
• Tracking: Courier tracking numbers (if applicable) and continuous possession logged (no unattended storage in vehicles or public spaces).

3. Transport Controls

• Physical controls: Locked cases; media on-person or in a locked vehicle compartment when brief stops are unavoidable; no overnight storage outside controlled facilities unless in approved safes/lockers.
• Route & Method: Pre-approved routes; reputable bonded courier service with evidence of security practices (if third-party used).
• Contingencies: If transport is interrupted, handler must notify security immediately, initiate containment, and document the incident.

4. Delivery & Receipt

• Verification: Recipient verifies identity, inspects seals, confirms encryption state for digital media, and signs chain-of-custody.
• Intake: Media moved directly into a controlled area; logged into inventory/CMDB if applicable.
• Decryption/Access: Per policy; only authorized recipients with business need; audit logging enabled for any access.

5. Post-Transport Review

• Record retention: Chain-of-custody logs retained per records policy.
• Exceptions/Incidents: Any deviation documented; security review conducted; corrective actions recorded.

Evidence Examples:

• Media Transport SOP/Policy:
• Defines authorized roles, encryption requirements (FIPS 140-2/140-3), packaging, approved couriers, and incident handling.
• Chain-of-Custody Documentation:
• Completed forms/logs showing end-to-end custody, seal IDs, signatures/time stamps, and encryption verification.
• Encryption Evidence (Digital Media):
• Screenshots showing BitLocker (or equivalent) FIPS-compliant encryption enabled; FIPS certificates for crypto modules; device status reports from MDM/endpoint management.
• Authorized Personnel & Training:
• Role roster and training records for staff permitted to transport CJI media.
• Transport Records & Receipts:
• Courier tracking logs, delivery confirmations, and intake logs at destination.
• Incident/Exception Reports:
• Documentation of any transport anomalies and remediation actions.

4. MP-6 MEDIA SANITIZATION
[Existing] [Priority 1]

Describe the agency's process for securely sanitizing or destroying CJI media when it is no longer needed (e.g., wiping, shredding, degaussing). Include the approved techniques and equipment used.

CJIS Requirement:

CJIS Security Policy § 5.8.4 – Media Sanitization requires agencies to sanitize or destroy media containing CJI before disposal or reuse. Sanitization must use approved techniques and equipment that renders data unrecoverable, consistent with NIST SP 800-88 Rev. 1 guidelines. Agencies must document the process and maintain records of sanitization or destruction.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Process Description (What the Auditor Should See)

1. Identification & Authorization
• Media flagged for disposal or reuse is identified in inventory.
• Disposal/sanitization request approved by data owner or IS/security officer.

2. Approved Sanitization Methods
• Digital Media:
• Cryptographic Erase: Securely delete encryption keys for encrypted drives.
• Secure Wipe: Overwrite using NIST-approved tools (e.g., DoD 5220.22-M, NIST 800-88 compliant software).
• Degaussing: For magnetic media (backup tapes, HDDs) using NSA/CJIS-approved degaussers.
• Physical Media:
• Shredding: Cross-cut shredders for paper documents.
• Pulverization or Incineration: For optical discs or other non-rewritable media.
• Physical destruction: Drilling, crushing, or shredding of drives after wipe/degauss.

3. Equipment & Tools
• Examples:
• Wiping software: Blancco, Active KillDisk, or built-in OS tools configured for NIST compliance.
• Degaussers: NSA-approved models (e.g., Garner HD-3WXL).
• Shredders: High-security cross-cut shredders (DIN 66399 Level P-5 or higher).

4. Documentation & Verification
• Sanitization Log includes:
• Media ID, type, serial number.
• Sanitization method used.
• Date/time.
• Technician name and signature.
• Verification step (e.g., wipe report, destruction certificate).
• Certificates of Destruction from third-party vendors (if applicable).

5. Chain-of-Custody
• Maintained from identification through destruction.
• Includes custody transfers and verification signatures.

Evidence Examples:

• Media Sanitization Policy/SOP:
• Specifies approved methods, equipment, and documentation requirements.
• Sanitization Logs:
• Completed forms showing media details, method, date, and verification.
• Certificates of Destruction:
• From internal process or third-party vendor.
• Equipment Records:
• Proof of NSA/CJIS-approved degaussers or shredders.
• Wipe Reports:

• Generated by sanitization software confirming compliance with NIST 800-88.

Section - Policy Area 9 - Physical Protection (PE)

1. PE-2 PHYSICAL ACCESS AUTHORIZATIONS
[Existing] [Priority 1]

Does the agency manage and review physical access to secure areas where CJIS systems are located?

CJIS Requirement:

CJIS Security Policy § 5.9.2 – Physical Access Authorizations requires agencies to authorize, manage, and review physical access to secure areas housing CJIS systems. Access must be limited to authorized personnel, documented, and reviewed at least annually. Agencies must maintain records of access authorizations and promptly revoke access when personnel no longer require it.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

- Physical Access Policy/SOP:
- Defines secure areas (server rooms, evidence rooms, network closets).
- Specifies authorization process, review frequency, and revocation procedures.
- Access Control Lists (ACLs):
- Current list of personnel authorized for secure areas.
- Role-based access assignments.
- Access Logs:
- Badge/keycard logs showing entries to secure areas.
- Audit reports of access activity.
- Annual Review Records:
- Documentation of access list review and updates.
- Evidence of removed access for terminated or transferred personnel.
- Training Records:
- Proof that authorized personnel completed physical security training.

○ Yes
○ No

Primary question answered Yes

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

☐ I have read and will comply.

2. PE-3 PHYSICAL ACCESS CONTROL
[Existing] [Priority 1]

How does the agency manage and enforce physical access controls for facilities containing CJIS systems or CJI?

Please describe:
• The procedures for verifying authorized personnel before granting entry
• How access is logged and audited
• Use of card readers, keys, biometrics, or physical barriers
• Visitor escort procedures
• How lost/stolen keys, transferred staff, or compromised codes are handled
• The process for annual access device inventory

CJIS Requirement:

CJIS Security Policy § 5.9.3 – Physical Access Control requires agencies to restrict and manage physical access to areas housing CJIS systems or CJI. Controls must ensure only authorized, vetted personnel can enter; all visitors are escorted; access events are logged and auditable; and keys/cards/codes are issued, inventoried, and revoked upon role changes or compromise. Combinations/codes must be changed upon personnel turnover or suspected exposure, and agencies must maintain documented procedures for access issuance, review, and device inventory.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Process Description (What the Auditor Should See)

1. Verification Before Entry
• Identity verification: Personnel must present a valid agency-issued photo badge; guards or reception validate identity against the current authorized access list (role-based).
• Two-person rule (where applicable): For highly restricted rooms (e.g., server room), dual verification or two-factor physical access (badge + PIN/biometric).
• After-hours protocols: Additional verification (e.g., supervisor approval, SOC notification) and logging.

2. Access Logging & Auditing
• Automated logs: Badge/card reader systems record time, user, door, result (granted/denied).
• Manual logs: Where keys or visitor access is used, entry/exit logs with date/time, purpose, escort, and destination are maintained.
• Audits: Logs are reviewed at least monthly (or per policy), with anomalies escalated to security; annual control audit verifies completeness and retention.

3. Controls & Barriers
• Card readers/PINs/biometrics: Deployed at entrances to server rooms, network closets, evidence rooms, and other CJIS areas.
• Physical barriers: Locked doors, cages, cabinet locks, turnstiles, and mantraps where appropriate; CCTV coverage with retention per records policy.
• Key management: Keys are numbered, checked out, and tracked; master keys are secured; spares are stored in sealed custody.

4. Visitor Escort Procedures
• Pre-approval: Visitor access approved by data/system owner or security; purpose and areas permitted documented.

• Sign-in/out: Visitors present ID, sign visitor log, receive temporary badge with distinct visual marking; escort is mandatory at all times.
• Restrictions: No unescorted access to CJIS areas; bags/equipment may be inspected; photography restricted per policy.

5. Exceptions & Incident Handling
• Lost/stolen keys/cards: Immediate reporting, deactivation of cards, rekeying/code changes if exposure is suspected; incident documented and reviewed.
• Transferred/terminated staff: Same-day revocation of physical access; return of keys/cards recorded.
• Compromised codes/combinations: Change codes promptly and document the change; notify impacted areas; review access lists.

6. Annual Access Device Inventory
• Inventory scope: All keys, access cards, fobs, PINs/codes, and biometric enrollments tied to CJIS areas.
• Reconciliation: Compare device records against current personnel roster and authorized access lists; identify orphans or stale assignments.
• Attestation: Security/Facilities sign off on the annual inventory, including remediation of discrepancies.

Evidence Examples:

• Physical Access Control Policy/SOP
• Defines secure areas, verification steps, logging/auditing cadence, visitor handling, incident response, and annual inventory procedure.
• Authorized Access Lists & Role Mapping
• Current list of personnel authorized for each secure area; mapping to job roles and vetting status.
• Access Logs & Audit Reports
• Badge reader exports (last 90 days), CCTV audit trail, visitor sign-in sheets, monthly/quarterly audit summaries and findings.
• Device & Credential Inventories
• Annual inventory reports of keys/cards/fobs/PINs/biometric enrollments; reconciliation results and remediation tickets.
• Incident/Revocation Records
• Tickets for lost/stolen keys/cards, code changes, and personnel transfer/termination revocations (with timestamps).
• Training Records
• Proof that authorized personnel and escorts completed physical security & visitor handling training.

3. PE-4 ACCESS CONTROL FOR TRANSMISSION
[Existing] [Priority 2]

Does the agency implement and enforce physical access controls to protect information system distribution lines, transmission cabling, and related devices inside agency facilities, ensuring only authorized personnel can access or interact with these components according to established agency procedures?

CJIS Requirement:

The agency must physically secure system distribution and transmission lines and associated devices within organizational facilities by implementing appropriate physical access controls—such as locked wiring closets, conduits, cable trays, locked spare jacks, and wiretapping sensors—to prevent damage, tampering, eavesdropping, or unauthorized modifications to

systems transmitting CJI.

Evidence Examples:

Policy or SOP defining:
• Requirements for locking or otherwise securing cabling and wiring infrastructure that transmit CJI (e.g., within conduit, cable trays, locked jacks, or locked wiring closets).
• Procedures requiring placement and use of physical safeguards (e.g., locks, sensors) on transmission line endpoints in all areas housing CJI equipment.
• Processes for inspecting or validating physical controls for transmission lines (e.g., quarterly reviews of wiring closet access and cabling integrity).

Facility and Physical Security Configurations:
• Photographs, floor plans, or diagrams showing locked wiring closets or secured racks containing transmission cabling.
• Documentation of conduit, cable trays, locked spare jacks, or physical enclosures protecting transmission pathways.
• Installation records or purchase orders proving deployment of wiretapping detection sensors or anti tamper mechanisms.

Access Control and Inspection Records:
• Physical access logs or badge-in/out records for personnel entering secured cabling areas.
• Maintenance or inspection logs showing annual or quarterly verifications of physical security controls for transmission infrastructure.
• Incident tickets or discrepancy reports detailing unauthorized access or damage to transmission lines and associated remedial actions.

Change Control and Monitoring:
• Change tickets authorizing installation or modification of cabling or transmission hardware.
• Audit logs or CCTV footage capturing access to secured cabling areas, and any unauthorized attempts recorded and responded to.

System Security Plan (SSP):
• Sections detailing the physical protection measures for transmission lines, including secured wiring closets, conduits, locked jacks, anti tamper sensors, and oversight mechanisms.
• Definitions of responsible roles (facilities personnel, physical security, ISSOs) for managing, inspecting, and maintaining PE 4 controls.

○ Yes
○ No

4. PE-6 MONITORING PHYSICAL ACCESS

How does the agency monitor and review physical access to secure areas where CJIS systems reside?

Please describe:
• Whether alarms, cameras, or surveillance systems are used
• How often physical access logs are reviewed (e.g., quarterly)
• How physical security incidents are documented and escalated
• How monitoring results are shared with the incident response team
• Who is responsible for managing and reviewing physical access records

CJIS Requirement:

CJIS Security Policy § 5.9 – Physical Security requires agencies to monitor and review physical access to secure areas where CJIS systems or CJI are present. Controls must include surveillance/monitoring mechanisms, logging of access events, documented review cadence, incident documentation and escalation, and coordination with incident response. This aligns with NIST SP 800 53 PE 6 (Monitoring Physical Access) and the broader CJIS physical access controls (PE 2/PE 3) to ensure only authorized access and timely detection/response to anomalies.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Process Description (What the Auditor Should See)

1. Monitoring Mechanisms in Secure Areas
• Surveillance systems: CCTV cameras covering entrances, egress routes, server rooms, network closets, evidence rooms, and any area housing CJIS systems; camera placement minimizes blind spots; retention per records policy (e.g., 30–90 days).
• Alarms & sensors: Door-forced-open alarms, door-held-open alerts, motion sensors after hours.
• Access control systems: Card readers, PIN pads, and/or biometrics; all access attempts (granted/denied) are logged.

2. Access Log Review Cadence
• Routine review: Badge reader logs, alarm events, and visitor logs are reviewed at least quarterly; high-risk areas (server rooms, data centers) reviewed monthly or weekly depending on risk.
• Exception-based review: After-hours entries, repeated denials, door-held alarms, or unusual access patterns trigger targeted review.
• Documentation: Each review produces a summary report (findings, anomalies, actions taken) with date/time and reviewer sign-off.

3. Incident Documentation & Escalation
• Classification: Physical security incidents categorized (e.g., unauthorized access attempt, tailgating, forced door, missing keys/cards).
• Recording: Incidents recorded in the security ticketing system with evidence (log snippets, camera screenshots, timestamps).
• Escalation path: Guard/reception Facilities/Security Information Security (IS)/SOC Incident Response (IR); time bound SLAs based on severity.
• Containment actions: Immediate measures (lockdown, card deactivation, code changes, escort to exit), followed by post incident review and corrective actions.

4. Sharing Results with Incident Response (IR)
• Automated feeds: Access control/alarm logs integrated to SIEM; alerts sent to SOC/IR mailbox or queue.
• Periodic briefings: Monthly/quarterly summaries of physical access monitoring provided to IR team; notable trends and remediation tracked to closure.
• Cross discipline correlation: IR correlates physical events (e.g., denied access) with logical security events (e.g., failed VPN login) for comprehensive investigations.

5. Roles & Responsibilities
• Facilities/Security Manager: Owns physical access systems (cameras, card readers), ensures maintenance and uptime.
• Information System Security Officer (ISSO)/CJIS Coordinator: Sets review cadence, receives reports, ensures CJIS alignment, coordinates with IR.
• SOC/IR Team: Monitors alerts, investigates incidents, leads response and post mortems.
• System/Area Owners: Validate authorized access lists, approve visitor access, and act on remediation recommendations.
• Records/Compliance: Maintains retention schedule and ensures audit readiness.

Evidence Examples:

• Physical Security & Monitoring Policy/SOP
• Defines surveillance coverage, alarm use, log retention, review frequency, incident classification, escalation, and reporting to IR.
• Access Control & Surveillance Artifacts
• Camera layout diagrams, retention settings screenshots, alarm configuration (door forced/held), card reader settings.
• Sample logs: Badge access logs (last 90 days), alarm event exports, visitor sign in sheets.
• Review Reports & Sign Offs
• Quarterly/Monthly review summaries with anomalies identified and actions taken; reviewer signatures and dates.
• Incident Records
• Tickets showing timeline, evidence (video stills, log entries), containment, notification to IR, and corrective actions.
• Integration Evidence

• SIEM rules/alerts for physical events; notification workflows; examples of IR case files with physical logical correlation.
• Responsibility Matrix (RACI)
• Document mapping who manages systems, who reviews, who approves, and who responds.

5. PE-17 ALTERNATE WORK SITE

Does the agency have any alternate worksite?

CJIS Requirement:

CJIS Security Policy § 5.9.6 – Alternate Work Sites requires agencies to ensure that any location outside the primary facility where CJI is accessed, processed, stored, or transmitted (e.g., telework sites, temporary offices, mobile command centers) meets physical and logical security requirements equivalent to those of the primary site. This includes physical access controls, encryption of CJI, secure network connectivity, and procedures for monitoring and incident response.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Process Description (What the Auditor Should See)

1. Authorization & Documentation
• Alternate work sites must be approved by the agency's security officer or CJIS coordinator.
• Documented in the agency's security plan, including location, purpose, and assigned personnel.

2. Physical Security Controls
• Controlled access: Locked doors, restricted entry, and visitor escort procedures.
• Secure storage: Lockable cabinets or safes for media and devices containing CJI.
• Environmental protections: No public access; signage indicating restricted area.

3. Logical Security Controls
• Encrypted connections: VPN with FIPS 140-2 or higher validated cryptographic modules for remote access.
• Device hardening: Agency-managed laptops or MDTs configured per CJIS standards (e.g., disk encryption, MFA, endpoint protection).
• No personal devices for CJI processing unless explicitly authorized and secured.

4. Monitoring & Incident Handling
• Access logs: Badge or key logs for alternate site entry; visitor logs maintained.
• Network monitoring: Remote sessions logged and reviewed; alerts for unauthorized access attempts.
• Incident response integration: Physical or logical security incidents at alternate sites reported to the IR team immediately.

5. Training & Awareness
• Personnel assigned to alternate sites receive CJIS security training, including physical and logical security requirements for remote locations.

Evidence Examples:

• Alternate Work Site Policy/SOP:
• Defines approval process, physical and logical security requirements, monitoring, and incident handling.
• Site Authorization Records:
• Documentation of approved alternate sites and assigned personnel.

• Physical Security Evidence:
• Photos of secure areas, access control systems, visitor logs.
• Logical Security Evidence:
• VPN configuration screenshots showing FIPS-compliant encryption.
• Device hardening reports (disk encryption, MFA, endpoint protection).
• Monitoring & Incident Records:
• Access logs, network session logs, and incident tickets related to alternate sites.
• Training Records:
• Proof of CJIS security training for personnel using alternate sites.

○ Yes
○ No

Primary question answered Yes

1. How does the agency manage, and secure alternate work sites used to process, store, and/or transmit CJI?

Please describe:

• How alternate locations are documented and approved
• What controls are in place to protect CJI at those locations (e.g., locks, encryption, limited access)
• How devices and documents are secured when unattended
• How staff report incidents or security concerns when working remotely
• Whether agreements or SOPs are in place for remote access and offsite CJI handling

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

1. SC-7 BOUNDARY PROTECTION

Describe how the agency protects the boundaries between internal CJIS systems and external networks. Include:

• How communications are monitored at key network interfaces (internal and external)
• Use of firewalls, intrusion detection/prevention systems (IDS/IPS), or other boundary protection tools
• How public-facing services are isolated from internal systems
• How external network access is restricted, logged, and reviewed
• Whether boundary protections are documented in the agency's security architecture

Provide evidence of these protections, such as network diagrams, firewall/IDS configurations, security architecture documentation, and logs showing monitoring and access reviews.

CJIS Requirement:

CJIS Security Policy § 5.10 — System and Communications Protection and Information Integrity requires agencies to implement technical and administrative controls to protect system boundaries, ensuring that communications to and from CJIS environments are filtered, monitored, and controlled. This includes use of firewalls, IDS/IPS, segmentation/DMZs, logging and review, and documented security architecture. The requirement aligns with NIST SP 800 53 SC 7 (Boundary Protection) and related controls (SC 5, SC 7(5), SC 7(12), SC 32), emphasizing separation of public-facing services from internal systems and restricting external access to least privilege.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Process Description (What the Auditor Should See)

1. Boundary Definition & Documentation
• CJIS vs. non CJIS zones defined in the security architecture (e.g., diagrams labeling trust boundaries, security zones, and interconnections).
• Data flow mapping for all ingress/egress paths (Internet, state CJIS/NCIC links, vendor interfaces, cloud connections).

2. Protection at Key Interfaces
• Firewalls at all Internet and WAN edges enforcing deny all, permit-by-exception rules; explicit egress filtering (only necessary outbound ports/protocols).
• IDS/IPS monitoring inline or via SPAN/TAP for north-south and east-west traffic in CJIS zones; signatures and behavioral analytics tuned to agency environment.
• Web Application Firewalls (WAF) and reverse proxies for public-facing apps; SSL/TLS termination with FIPS validated crypto for CJI-related services.
• DNS security controls (RPZ/DNS filtering), email gateways with anti malware/anti phishing, and content filters for outbound data exfiltration controls.

3. Segregation & Isolation of Public Services
• DMZs (or isolated subnets) host public-facing services (web portals, email relay, SFTP endpoints); no direct lateral paths into CJIS internal networks.
• Network segmentation (VLANs, VRFs) separates CJIS servers, endpoints, and admin networks; access control lists (ACLs) enforce least privilege between segments.
• Bastion hosts/jump boxes mediate administrative access; no direct RDP/SSH from external networks to internal CJIS systems.

4. External Access Restrictions, Logging, and Reviews
• External access granted only via VPN or Zero Trust gateways with MFA, device posture checks, and FIPS 140 2/ 3 validated crypto.
• Comprehensive logging: firewall allows/denies, IDS/IPS alerts, VPN session logs, WAF events, proxy transactions. Logs are centralized in SIEM and retained per policy.
• Review cadence: weekly or monthly review of boundary logs; quarterly control reviews of firewall rules/ACLs; annual architecture review and risk assessment.

5. Monitoring & Response Integration
• Continuous monitoring with alerting on suspicious patterns (port scans, repeated denies, unusual egress, geo anomalies).
• Alerts escalated to SOC/IR, correlated with endpoint and identity telemetry; playbooks guide containment (block rules, session termination, segmentation changes).

6. Change & Configuration Governance
• Documented change control for boundary rules, with risk assessment, approvals, and post implementation validation.
• Baseline configurations (CIS/DISA) applied to firewalls, routers, IDS/IPS, and WAF; backup & version control maintained for configs.

Evidence Examples:

• Network & Security Architecture Documentation
• Current network diagram showing CJIS/non CJIS boundaries, DMZs, VLANs, trust zones, and all boundary devices (firewalls, IDS/IPS, WAF, proxies).
• Data flow diagrams for public services, VPN, cloud integrations, and state CJIS connections.
• Boundary Device Configurations & Screenshots
• Firewall rule exports (with change history), NAT policies, and egress controls.
• IDS/IPS policies and alert dashboards (signatures, tuning notes).
• WAF policies (OWASP rulesets, TLS settings), reverse proxy configs.
• VPN gateway settings (MFA enforced; cipher suites; FIPS mode enabled).
• Monitoring & Review Artifacts
• SIEM dashboards and weekly/monthly log review reports (findings, actions).
• Quarterly firewall/ACL review records with approvals and remediation.
• Incident tickets showing detection, escalation, containment, and lessons learned.
• Control Baselines & Governance
• CIS/DISA-aligned hardening baselines for boundary devices; config backups/version control logs.

• Change management tickets for boundary updates with approvals and validation evidence.

2. SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Describe how the agency ensures the confidentiality and integrity of CJI during transmission over internal and external networks. Include:

- Cryptographic protections in place (e.g., VPN, TLS, FIPS 140-2 validated)
- How endpoints such as laptops, scanners, and radios are protected during transmission
- Whether commercial internet or cloud-based systems are used, and how they are secured
- How unauthorized access or modification during transmission is detected or prevented
- How metadata derived from CJI is handled, especially when using cloud providers or third-party services

Provide evidence of these protections, such as network diagrams, encryption configurations, VPN/TLS settings, security architecture documentation, and monitoring logs.

CJIS Requirement:

CJIS Security Policy § 5.10.1 – System and Communications Protection requires agencies to implement cryptographic mechanisms to protect the confidentiality and integrity of CJI during transmission across internal and external networks. All cryptographic modules must be FIPS 140-2 or higher validated. This applies to VPNs, TLS sessions, wireless communications, and any data exchange with cloud or third-party services. Agencies must also ensure metadata handling does not expose sensitive information and must monitor for unauthorized access or modification during transmission.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Process Description (What the Auditor Should See)

1. Cryptographic Protections
- VPN: All remote access and site-to-site connections use IPsec or SSL VPN with FIPS 140-2 validated cryptographic modules, enforcing AES-256 encryption and SHA-2 integrity checks.
- TLS: Internal and external web services use TLS 1.2 or higher with FIPS-compliant cipher suites; weak protocols (SSL, TLS 1.0/1.1) disabled.
- Wireless: WPA2-Enterprise or WPA3 with 802.1X authentication and FIPS-compliant encryption for MDTs and agency laptops.
- Endpoints: Laptops and MDTs configured for full-disk encryption, secure VPN clients, and certificate-based authentication.

2. Commercial Internet & Cloud Security
- Cloud services (e.g., CJIS-compliant SaaS or IaaS) must be CJIS-certified or meet contractual security requirements.
- Data in transit to cloud providers encrypted using TLS 1.2+ and FIPS-validated modules.
- Metadata handling: Ensure logs, headers, and telemetry do not expose CJI; apply data minimization and tokenization where possible.

3. Detection & Prevention of Unauthorized Access
• Monitoring: IDS/IPS and SIEM monitor encrypted traffic patterns for anomalies; VPN logs reviewed for unauthorized attempts.
• Integrity checks: TLS and IPsec enforce cryptographic integrity; alerts generated for handshake failures or certificate issues.
• Access control: MFA enforced for all remote sessions; device posture checks before VPN connection.

4. Metadata Protection
• Headers and routing info sanitized; no CJI in URLs or query strings.
• Cloud logging reviewed to ensure compliance with CJIS data handling requirements.

Evidence Examples
• Network diagrams showing encrypted paths (VPN tunnels, TLS endpoints, wireless security zones).
• VPN configuration screenshots:
• FIPS mode enabled.
• Cipher suite settings (AES-256, SHA-2).
• TLS configuration evidence:
• Web server settings showing TLS 1.2+ enforced.
• Disabled weak protocols.
• Wireless security configs:
• WPA2-Enterprise/WPA3 settings.
• 802.1X authentication details.
• Cloud compliance documentation:
• CJIS compliance attestation or contract clauses.
• Monitoring logs:
• VPN session logs.
• IDS/IPS alerts for transmission anomalies.
• SIEM dashboards showing encrypted traffic monitoring and integrity alerts.

3. SC-13 CRYPTOGRAPHIC PROTECTION

Describe how the agency ensures encryption meets CJIS requirements when transmitting CJI outside of a physically secure location.

Include:

• What type of system(s)/network segment is involved
• When and how encryption is required for data in transit
• What cryptographic protocols or tools are used (e.g., TLS, IPsec, VPN)
• Whether FIPS 140-2/140-3 validated modules are used
• Key strength for symmetric encryption (e.g., AES 128-bit or higher)

Provide evidence of these protections, such as encryption configuration screenshots, VPN/TLS settings, FIPS validation documentation, and security architecture diagrams.

CJIS Requirement:

CJIS Security Policy § 5.10.1 (System and Communications Protection) and § 5.6/5.5 (Access Control) require the use of FIPS 140-2 or FIPS 140-3 validated cryptographic modules to protect the confidentiality and integrity of CJI during transmission whenever data leaves a physically secure location (e.g., telework, mobile, cloud exchanges, inter-agency links). This includes VPN (IPsec/SSL), TLS-protected applications, and wireless links involving CJI. Agencies must enforce approved cipher suites (e.g., AES-128 or stronger, SHA-2 integrity), disable legacy protocols, and document the protections in the security architecture.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Process Description (What the Auditor Should See)

1. Scope: Systems & Network Segments Involved
• Endpoints: Laptops, MDTs, tablets, scanners, radios, LiveScan devices.
• Application tiers: Web portals, RMS/CAD, evidence systems, email gateways, SFTP endpoints.
• Network segments: External Internet-facing paths, site to site links (partner/state CJIS), remote access segments, Wi Fi networks, cloud interconnects.

2. When & How Encryption Is Required (Data in Transit)
• Mandatory encryption whenever CJI is transmitted outside a physically secure location or across untrusted networks (Internet, public Wi Fi, partner networks).
• Internal encryption for sensitive east west traffic where links traverse mixed trust segments or wireless.
• Enforcement points: VPN gateways (remote access & site to site), application servers (TLS), email/file transfer services (TLS/S/MIME/SFTP), wireless controllers (WPA2 Enterprise/WPA3).

3. Cryptographic Protocols/Tools Used
• VPN/IPsec: IKEv2 with AES 256 (or AES 128 minimum), SHA 256/384 integrity, PFS/DH Group ≥14; tunnel mode for remote access and site to site.
• TLS (1.2 or 1.3): Server and client configurations enforce FIPS approved cipher suites (e.g., TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 or TLS 1.3 equivalents); legacy SSL/TLS 1.0/1.1 disabled.
• Wireless: WPA2 Enterprise/WPA3 Enterprise with 802.1X (EAP TLS), using certificates issued by a trusted CA; data plane encryption meets FIPS requirements.
• File/Email: S/MIME or TLS only mail transport; SFTP/FTPS for file exchange; CJIS approved secure messaging for radios/MDTs where applicable.

4. FIPS 140 2/140 3 Validation
• All cryptographic operations use FIPS validated modules (OS crypto libraries, VPN client/gateway, HSM/WAF/NGFW).
• FIPS mode enabled on platforms that support it (Windows, vendor appliances, specific crypto libraries).
• Maintain NIST CMVP certificate copies for the crypto modules in use and reference them in the security architecture.

5. Key Strength & Cryptographic Parameters
• Symmetric encryption: AES 128 (minimum), AES 256 preferred.
• Integrity/MAC: SHA 256 or higher.
• Key exchange: ECDHE or DH groups meeting FIPS strength; PFS required for VPNs/TLS.
• Certificates: Minimum 2048 bit RSA or ECC (P 256 or stronger); strong PRNG from FIPS validated module.

6. Detection/Prevention of Unauthorized Access or Modification During Transmission
• Mutual authentication (certificates/MFA) for VPN and administrative sessions.
• Certificate pinning/strict validation; HSTS for web; reject weak ciphers.
• Monitoring: SIEM ingests VPN/TLS handshake logs, firewall denies, IDS/IPS alerts (e.g., protocol downgrade attempts, anomalous session behavior).
• Automated policy checks: Regular scans to verify cipher profiles and detect drift.

7. Metadata Handling (Cloud/Third Party)
• Minimize metadata (no CJI in URLs/query strings/headers).
• Log redaction/tokenization for cloud telemetry; restrict sharing to least necessary.
• Contractual controls: Ensure providers commit to CJIS-compliant handling of telemetry/metadata and use FIPS validated crypto for transport.

8. Documentation & Governance
• Protections are documented in the security architecture, Network Security SOP, and Remote Access Policy; quarterly reviews verify cipher suites/FIPS status; change control governs crypto settings updates.

Evidence Examples:

• Security architecture diagrams showing encrypted paths (VPN tunnels, TLS endpoints, wireless segments) and trust boundaries.
• VPN configuration screenshots: IKEv2, AES 256/SHA 2, DH group, FIPS mode enabled; MFA posture checks.
• TLS server/client settings: Protocols TLS 1.2/1.3 only, allowed cipher suites, HSTS, certificate details (RSA 2048+/ECC).
• Wireless controller configs: WPA2/3 Enterprise, 802.1X (EAP TLS), RADIUS policies.
• FIPS validation documentation: NIST CMVP certificate PDFs or URLs for crypto modules (OS, VPN appliance, HSM).
• Monitoring logs: SIEM dashboards showing VPN/TLS events, IDS/IPS detections, policy compliance reports; quarterly review sign offs.
• Policies/SOPs: Remote Access, Transmission Security, Metadata Handling (with FIPS references and enforcement steps).

4. SC-28 PROTECTION OF INFORMATION AT REST

Does the agency store CJI outside of the secured location?

CJIS Requirement:

CJIS Security Policy § 5.10.1.3 – Protection of Information at Rest requires that CJI stored outside a physically secure location (e.g., laptops, MDTs, portable drives, cloud storage) must be encrypted using FIPS 140-2 or FIPS 140-3 validated cryptographic modules. Agencies must also implement secure key management practices to protect encryption keys from unauthorized access or disclosure.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Process Description (What the Auditor Should See)

1. Scope: Where CJI Is Stored Outside Secure Areas
• Endpoints: Laptops, MDTs, tablets, USB drives, backup tapes.
• Cloud storage: CJIS-compliant SaaS or IaaS platforms.
• Portable media: DVDs/CDs, external hard drives.

2. Encryption Methods
• Full-disk encryption (FDE) on laptops and MDTs using BitLocker, FileVault, or equivalent with FIPS mode enabled.
• Removable media encryption: USB drives encrypted with FIPS-validated tools (e.g., BitLocker To Go, hardware-encrypted drives).
• Cloud storage encryption: Data encrypted at rest using AES-256 or AES-128 minimum, with FIPS-validated modules.
• Database encryption: Transparent Data Encryption (TDE) for CJIS-related databases.

3. FIPS Validation
• All cryptographic modules used for encryption must be FIPS 140-2 or 140-3 validated.
• Maintain NIST CMVP certificates for OS crypto libraries, endpoint encryption tools, and cloud provider modules.
• Ensure FIPS mode is enabled on Windows/macOS/Linux endpoints and validated on vendor appliances.

4. Key Management Practices
• Centralized key management using enterprise tools (e.g., Microsoft MBAM, Azure Key Vault, AWS KMS, on-prem HSM).
• Separation of duties: Key custodians differ from system admins.
• Rotation and lifecycle management: Keys rotated per policy; retired keys securely destroyed.
• Access control: MFA and RBAC for key management systems.
• Audit logging: All key access and operations logged and reviewed.

5. Monitoring & Compliance
• Endpoint compliance reports: Show encryption status and FIPS mode enabled.
• Cloud compliance attestation: Vendor documentation confirming CJIS and FIPS adherence.
• Quarterly reviews: Validate encryption coverage and key management logs.

Evidence Examples:

• Encryption configuration screenshots:
• BitLocker status with FIPS mode enabled.
• FileVault or Linux LUKS settings.
• Cloud provider documentation:
• CJIS compliance statement and FIPS validation details.
• FIPS certificates:
• NIST CMVP listings for cryptographic modules used.
• Key management evidence:
• Screenshots of key vault settings, rotation schedules, and RBAC configurations.
• Monitoring reports:
• Endpoint encryption compliance dashboards.
• Logs showing key access and lifecycle events.
• Security architecture diagrams:
• Highlighting encrypted storage zones and key management components.

○ Yes
○ No

Primary question answered Yes

1. If yes, describe how CJI is protected at rest, including encryption methods, FIPS 140-2/140-3 validation, and key management practices.

2. Provide evidence of these protections, such as encryption configuration documentation, FIPS validation certificates, and security architecture diagrams.

☐ I have read and will comply.

Section - Policy Area 12 - Personnel Security

1. 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?

CJIS Requirement:

CJIS Security Policy § 5.12.1 requires agencies to screen and authorize personnel who need unescorted access to unencrypted CJI. This includes:

- Completing required background checks (fingerprint-based, state and national criminal history).
- Documenting authorization and maintaining an up-to-date list of individuals granted unescorted access.
- Reviewing and updating the list at least annually or upon personnel changes.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Process Description (What the Auditor Should See)

1. Screening & Authorization
- Personnel undergo fingerprint-based background checks per CJIS standards before access is granted.
- Authorization documented by the CJIS Security Officer (CSO) or designated authority.

2. Maintaining the Authorized List
- List includes:
- Full name
- Job title/role
- Date of background check completion
- Date of authorization
- Areas of access (e.g., server room, evidence storage)

- Stored securely and updated promptly when:
- Personnel leave or transfer
- Access requirements change
- Background check expires or fails

3. Review & Audit
- Annual review of the list for accuracy.
- Cross-check against HR roster and access control systems.
- Documented sign-off by CSO or compliance officer.

Evidence Examples:

- Authorized Personnel List:
- Current, dated within the last 12 months.
- Includes all required fields (name, role, authorization date).
- Background Check Records:
- Fingerprint-based checks completed and documented.
- Review Documentation:
- Annual review report or sign-off sheet.
- Access Control Integration:
- Badge system or physical access logs aligned with authorized list.

○ Yes
○ No

Primary question answered Yes

1. Provide evidence of this list, such as a redacted copy showing authorized personnel, review logs, or system records demonstrating compliance.

☐ I have read and will comply.

2. 5.12.4 Personnel Sanctions

Has the agency documented and communicated a formal disciplinary process that specifies sanctions for personnel who fail to comply with CJIS Security Policy or mishandle Criminal Justice Information (CJI), and can provide a copy of the local policy reflecting this process to the auditor for review?

CJIS Requirement:

CJIS Security Policy § 5.12.4 – Personnel Sanctions requires agencies to establish and document a formal disciplinary process that outlines sanctions for employees who:

- Fail to comply with CJIS Security Policy requirements.
- Mishandle or improperly access Criminal Justice Information (CJI).

The policy must be communicated to all personnel, enforced consistently, and available for auditor review.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

- Personnel Sanctions Policy:
- Standalone document or section in the agency's security policy.
- Includes violation categories, sanction levels, and escalation steps.
- Acknowledgment Records:
- Signed forms or electronic attestations from staff.
- Training Materials:
- Security awareness training that includes sanctions overview.
- Incident Records:
- Examples of enforcement (with sensitive details redacted).
- Annual Review Documentation:
- Sign-off showing policy was reviewed and updated.

○ 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.

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

1. SA-9 EXTERNAL SYSTEM SERVICES

Does the agency:

1. Ensure external service providers comply with CJIS Security Policy and include appropriate agreements (e.g., Management Control Agreement, CJIS Security Addendum, Outsourcing Standards) when applicable?
2. Define and document roles, responsibilities, and oversight for external service providers?
3. Monitor compliance through audits and inspections, including:
• Triennial audits of providers with CJI access as required by CJIS Policy
• Authority for unannounced inspections
• Sharing audit results with other CSAs as needed • Ongoing monitoring of provider compliance

CJIS Requirement:

CJIS Security Policy § 5.14 System and Services Acquisition mandates:

• Compliance by External Providers: Agencies must ensure external service providers comply with CJIS Security Policy requirements.
• Required Agreements:
• Management Control Agreement (MCA) for NCJAs performing criminal justice functions.
• CJIS Security Addendum for private contractors accessing CJI.
• Outsourcing Standards for Channelers and Non-Channelers handling CJI.
• Oversight and Roles: Agencies must define and document roles and responsibilities for managing external services.
• Monitoring and Audits: Agencies must monitor compliance through triennial audits, allow unannounced inspections, and share audit results with CSAs as needed.

Evidence Examples:
• Copies of Agreements:
• Signed MCA for NCJA relationships.
• Signed CJIS Security Addendum for contractors.
• Outsourcing Standard documentation for Channelers/Non-Channelers.
• Oversight Documentation:
• Policy or SOP defining roles and responsibilities for external service oversight.
• Audit Evidence:
• Triennial audit reports of external providers.
• Records of unannounced inspections or compliance checks.
• Monitoring Records:
• Logs or reports showing ongoing compliance verification.

○ Yes
○ No

2. SA-22 UNSUPPORTED SYSTEM COMPONENTS
[Priority 1] - [DPS Enhanced Priority 1]

Does the agency:
a. Replace system components when support from the developer, vendor, or manufacturer is no longer available; or
b. Provide alternative sources for continued support for unsupported components (e.g., original manufacturer support or original contracted vendor support)?

CJIS Requirement:

CJIS Security Policy § 5.14 – System and Services Acquisition (SA-22) requires agencies to manage unsupported system components to reduce security risks. When vendor/manufacturer support ends (e.g., no security patches, updates, or technical assistance), agencies must:

• Replace the component with a supported version; or
• Provide alternative support mechanisms, such as extended vendor contracts or third-party maintenance, ensuring continued security updates and compliance.

Status: Existing requirement, Priority 1 and DPS Enhanced Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

• System Inventory Report:
• Includes lifecycle dates and support status.
• Replacement Plans:
• Upgrade schedules and project documentation.
• Support Agreements:
• Extended vendor support or third-party maintenance contracts.
• Risk Assessment Reports:
• Documented analysis and compensating controls for unsupported components.
• Policy/SOP:
• Defines process for handling unsupported components.
• Annual Review Records:
• Sign-off showing inventory and support status were reviewed.

○ Yes
○ No

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

1. SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
[Existing] [Priority 1]

Does the agency:
a. Receive system security alerts, advisories, and directives from external sources (e.g., CISA, MS-ISAC, US-CERT, hardware/software vendors, federal/state advisories) on an ongoing basis?
b. Generate internal security alerts, advisories, and directives as necessary?
c. Disseminate security alerts, advisories, and directives to personnel responsible for implementing, operating, maintaining, and using the system?
d. Implement security directives within established time frames or notify the issuing organization of any noncompliance?

CJIS Requirement:

CJIS Security Policy § 5.10.4 – System and Information Integrity requires agencies to:

- Subscribe to and monitor external security advisories (CISA, MS-ISAC, US-CERT, vendor bulletins).
- Generate internal alerts when threats or vulnerabilities impact agency systems.
- Disseminate alerts and directives promptly to relevant personnel (IT, security, operations).
- Implement required actions within defined time frames or formally report noncompliance to the issuing authority.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Evidence Examples:

- Policy/SOP:
- Defines process for receiving, evaluating, and disseminating alerts.
- Subscription Proof:
- Email subscription confirmations for CISA, MS-ISAC, US-CERT.
- Internal Alert Records:
- Copies of advisories sent to staff.
- Change Management Tickets:
- Showing implementation of directives.
- Compliance Reports:
- Timeliness of patching and remediation.
- Training Records:
- Staff awareness of alert handling procedures.

○ Yes
○ No

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.

In addition, it is highly recommended the agency LASO subscribe to the DPS CJIS Security Office Technical Listserv, DIR, US-CERT that's available at:

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

2. SI-2 FLAW REMEDIATION
[Existing] [Priority 1]

Does the agency identify, track, and correct system flaws; test software and firmware updates for effectiveness and potential side effects before deployment; install security-relevant updates within the required timelines (Critical – 15 days, High – 30 days, Medium – 60 days, Low – 90 days); and ensure that flaw remediation activities are incorporated into the agency's configuration management process in accordance with established procedures?

CJIS Requirement:

Agencies must identify, report, and correct system flaws affecting applications, services, firmware, or software used to process, store, or transmit Criminal Justice Information (CJI). They must test related updates for effectiveness and unintended side effects before deployment, install security-relevant updates within defined timelines based on severity (Critical – 15 days; High – 30 days; Medium – 60 days; Low – 90 days), and integrate all flaw remediation activities into the agency's configuration management process.

Status Existing requirement, Priority 1

Evidence Examples:

Policy or SOP defining:
• Criteria and processes for identifying and reporting system flaws (including CJI-specific systems).
• Severity classification and update timelines tied to flaw criticality (Critical/High/Medium/Low).
• Protocols for pre-deployment testing of updates and firmware (test plans, approval gates).
• Procedures for integrating patching actions into configuration management workflows (change requests, version control).

Flaw Identification & Reporting Records:
• Vulnerability scan reports or CVE/CWE tracking logs flagging discovered flaws.
• Tickets or reports forwarded to designated security/configuration personnel.
• Logs from continuous monitoring or incident response showing flaw findings.

Update Testing Records:
• Testing plans with scope, test results, and approval signatures.
• Documentation on rollback procedures and observed side effects during test cycles.
• Risk acceptance or change approval forms.

Update Installation Records with Timeliness:
• Patch management system export showing approved updates installed within required days.
• System logs or endpoint management reports with timestamps aligning to severity timelines.
• Change control tickets detailing rollback instructions and validation steps.

Configuration Management Integration Artifacts:
• Change request records including flaw remediation elements.
• Baseline configuration documentation reflecting applied updates.
• Version-controlled configuration items and audit logs.

Monitoring & Validation Evidence:
• Dashboards or automated reports showing patch status by severity.
• Periodic audit logs confirming that updates applied and no regression occurred.
• Incident follow-ups where flaw remediation was tracked and confirmed as part of CM records.

○ Yes
○ No

3. SI-3 MALICIOUS CODE PROTECTION[Existing] [Priority 1]

Does the agency implement and maintain malicious code protection mechanisms that provide signature-based detection at system entry and exit points; automatically update anti-malware definitions in accordance with configuration management procedures; perform daily scans and real-time scanning of files from external sources across servers and endpoint devices; block or quarantine detected malicious code and alert appropriate security personnel; and address false positives in a manner that prevents unnecessary disruption to system availability?

CJIS Requirement:

Agencies must implement malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code. These mechanisms must:

- Be signature-based (and optionally non-signature-based/heuristic)
- Automatically receive updates in line with configuration management procedures
- Perform daily periodic scans of the system and real-time scans of external files at network and endpoint entry/exit points
- Block or quarantine detected malicious code, trigger incident response procedures, and generate alerts to appropriate security personnel
- Address false positives to prevent unintended disruption to system availability
- Apply controls across all systems processing, storing, or transmitting Criminal Justice Information (CJI), including servers, workstations, mobile devices, firewalls, remote access servers, email and web servers, and proxy devices

Evidence Examples:

Policy or SOP defining:
- Signature-based (and optional heuristic) malicious code protection requirements at system entry/exit points
- Timely automatic updates of malware definitions in line with CM policy
- Scan schedules: daily full scans plus real-time/ on-access scans for external files across all platforms
- Actions for detected malicious code: block, quarantine, incident escalation, and alerting
- Procedures for handling false positives to avoid unnecessary system disruption
- List of systems and roles responsible for implementation, alerting, and false positive management

Malware Protection System Configuration & Updates:
- Endpoint security/antivirus dashboard or tool output showing signature-based scanning deployed at system boundaries
- Configuration screenshots or exports showing scheduled daily scans and real-time scanning settings
- Configuration management or patch system logs demonstrating automatic signature updates
- Logs from remediation actions (quarantine/block events) tied to incident response and ticket generation

Detection & Alerting Logs:
- Alert records identifying malicious code with time stamps, affected system, and remediation status
- Incident response initiation tickets and communication logs (email, SIEM) sent to security/ network teams following detection

False Positive Management Records:
- Tickets or log entries documenting false positive incidents, actions taken, and system availability outcome
- Communications or SOP notes describing escalation or exemption procedures to mitigate false positives

System Inventory & Boundary Coverage:
- Asset lists identifying systems with deployed malicious code protection (servers, endpoints, network entry devices)
- Deployment validation reports or scans confirming protection on all required devices

System Security Plan (SSP):
- Sections describing SI-3 implementation: types of protection, update mechanisms, scan schedules, alerting roles, false positive handling
- Diagrams or narratives showing deployment across all system entry and exit points

○ Yes
○ No

Section - Policy Area 19 - Risk Assessment (RA)

1. RA-2 SECURITY CATEGORIZATION

Has the agency:

1. Categorized each information system and the information it processes, stores, and transmits in accordance with applicable standards (e.g., CJIS Security Policy)?
2. Documented the security categorization results and supporting rationale in the system's security plan?
3. Ensured the authorizing official (or designated representative) has reviewed and approved the categorization decision?

CJIS Requirement:

CJIS Security Policy § 5.10.3 requires agencies to categorize systems and associated information in accordance with FIPS 199 and CJIS guidelines. This includes documenting the categorization results and rationale in the SSP and obtaining formal approval from the Authorizing Official (AO) or designated representative.

Status: Existing requirement, Priority 2 in the CJIS Requirements Companion.

Evidence Examples:

- Policy or SOP defining:
- Categorization methodology (FIPS 199/CJIS).
- Roles responsible for categorization and approval.
- Review and update frequency.
- System Security Plan (SSP):
- Categorization results for each system.
- Supporting rationale for confidentiality, integrity, and availability impact levels.

- AO or designated representative's signature/date approving categorization.
- FIPS 199 Worksheets:
- Completed worksheets showing impact ratings for systems.
- Approval Records:
- Signed forms or electronic approvals from AO.
- Meeting minutes or documented decision logs.
- Governance Artifacts:
- Categorization checklist integrated into system onboarding.
- Evidence of periodic recategorization after major changes.

○ Yes
○ No

2. RA-3 RISK ASSESSMENT

Does the agency conduct risk assessments for information systems at planned intervals and when significant changes occur, identifying threats, vulnerabilities, and potential impacts to determine risk levels?

CJIS Requirement:

CJIS Security Policy § 5.10.3 requires agencies to perform formal risk assessments to identify and evaluate risks to systems processing Criminal Justice Information (CJI). Assessments must consider threats, vulnerabilities, and likelihood/impact, and results must inform security planning and control selection.

Status: Existing requirement, Priority 2 in the CJIS Requirements Companion.

Evidence Examples:

• Policy or SOP defining:
• Risk assessment methodology (e.g., NIST SP 800 30).
• Frequency of assessments and triggers for reassessment.
• Roles responsible for conducting and approving assessments.
• Risk Assessment Reports:
• Documented threats, vulnerabilities, and impact analysis.
• Risk ratings and prioritization.
• Recommendations for mitigation.
• System Security Plan (SSP):
• References to completed risk assessments.
• Integration of risk results into control selection.
• Meeting Minutes or Approval Records:
• AO or security team review and acceptance of risk assessment results.
• Change Management Records:
• Evidence of risk reassessment after major system changes.

○ Yes
○ No

3. RA-5 VULNERABILITY MONITORING AND SCANNING
[Priority 1]

Does the agency:
a. Monitor and scan for vulnerabilities in systems and hosted applications at least monthly and when new vulnerabilities are identified and reported?
b. Use vulnerability monitoring tools and techniques that:
Enumerate platforms, software flaws, and improper configurations; Format checklists and test procedures; Measure vulnerability impact;
c. Analyze vulnerability scan reports and monitoring results?
d. Remediate legitimate vulnerabilities within the following time frames:
- Critical – 15 days
- High – 30 days
- Medium – 60 days
- Low – 90 days

e. Share vulnerability monitoring and assessment information with personnel responsible for risk assessment and control implementation to prevent similar vulnerabilities in other systems?
f. Employ vulnerability monitoring tools that can readily update vulnerability definitions?

CJIS Requirement:

CJIS Security Policy § 5.10 – System and Information Integrity (aligned to NIST SP 800 53 RA 5) requires agencies to conduct regular vulnerability monitoring and scanning, analyze results, remediate findings within defined time frames, and share outcomes with risk and control owners to prevent recurrence. Tools must be kept current (updated signatures/plugins) and scans must also occur when new significant vulnerabilities are announced or after major changes.

Status: Existing requirement, Priority 1 in the CJIS Requirements Companion.

Process Description (What the Auditor Should See)

1. Scanning Cadence & Triggers
• Monthly authenticated scans for servers, endpoints, network devices, web applications, and cloud resources.
• Out of band scans triggered by: high profile CVEs, vendor advisories, system changes, or incidents.
• Scope includes internal networks, perimeter systems, and externally exposed services.
2. Tools & Techniques
• Enterprise scanners (e.g., Tenable/Nessus, Rapid7 InsightVM, Qualys) for OS/app/config vulnerabilities.
• Web app scans (e.g., AppScan/Burp/Qualys WAS) and configuration benchmarks (e.g., CIS-CAT/SCAP).
• Authenticated scanning and agent-based telemetry to enumerate platforms, flaws, and misconfigurations.
• Use of standardized checklists/test procedures and severity metrics (CVSS based) to measure impact.
3. Analysis & Triage
• Security team reviews reports to validate true positives, de-duplicate, and assign risk ratings.
• Findings routed via ticketing system to asset owners with due dates per severity.
• False positives documented; compensating controls recorded if remediation isn't feasible.
4. Remediation SLAs (from your policy)
• Critical: 15 days | High: 30 days | Medium: 60 days | Low: 90 days.
• Emergency changes follow expedited change control; standard changes follow normal CAB process.
• Post remediation verification scans confirm closure.
5. Sharing & Governance
• Results shared with Risk Management, System Owners, and Control Implementers; trends reported to leadership.
• Persistent issues trigger root cause analysis and control enhancements (e.g., hardening updates, patch process improvements).
• Metrics tracked: time-to-remediate, open findings by severity, scan coverage, SLA adherence.
6. Tool Currency & Content Updates

• Scanners configured for daily plugin/signature updates.
• Threat intelligence feeds integrated where applicable; change logs retained.

Evidence Examples:

• Vulnerability Management SOP/Policy:
• Specifies monthly scan cadence, triggers for out-of-band scans, scope, authenticated scanning, analysis workflow, and remediation SLAs.
• Scanner Configuration & Reports:
• Screenshots showing scan schedules, authentication settings, plugin update status.
• Recent monthly reports with asset coverage and severity breakdown.
• Ticketing & Remediation Records:
• Tickets showing assignment, remediation actions, dates, and verification scan closure.
• SLA dashboards (Critical/High/Medium/Low) and compliance rates.
• Benchmark/Compliance Evidence:
• CIS/SCAP scan results; configuration hardening reports tied to vulnerability findings.
• Risk & Sharing Artifacts:
• Quarterly vulnerability trend reports shared with risk and control owners.
• Meeting minutes or distribution logs to stakeholders.
• Change Management Evidence:
• CAB approvals for patches/mitigations; emergency change logs for Critical issues.

○ Yes
○ No
○ n/a

Primary question answer 1 selected

1. (2) VULNERABILITY MONITORING AND SCANNING | UPDATE VULNERABILITIES TO BE SCANNED
[Priority 1]

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

○ Yes
○ No

2. (5) VULNERABILITY MONITORING AND SCANNING | PRIVILEGED ACCESS
[Priority 1]

Does the agency:
Implement privileged access authorization to information system components containing or processing CJI for vulnerability scanning activities requiring privileged access?

○ Yes
○ No

3. (11) VULNERABILITY MONITORING AND SCANNING | PUBLIC DISCLOSURE PROGRAM
[Priority 1]

Does the agency:
Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components?

○ Yes
○ No

Section - Final Documentation Acknowledgment

1. Has the agency provided all supporting documentation needed to support their responses during the audit?

Checklist includes:

• Interagency/Interlocal Agreements
• Signed Management Control Agreement for technical or dispatch services (MCA)
• Signed Security Addendums (all personnel/vendors with CJI access)
• Incident Response Policy and Procedures
• Security Incident Logs
• Auditing and Accountability Policy and Procedures
• Audit Logs (SIEM Tool Report), Patch Reports, Antivirus/Encryption settings
• Logical & Physical Access Control List
• User Access Roster (CJIS users, roles, last access, privilege level)
• Remote Access Policy and Procedures
• Current Network/System Diagram (firewalls, switches, servers, CAD, RMS, Livescan, backup, etc.)
• System Component Inventory Equipment List /Mobile/Bluetooth device inventories
• Media Protection Policies and step by step procedures (media storage, media transport, media sanitization, etc.)
• Systems and Communications Protection (FIPS certificates for CJI access, transmit, and at rest)
• Personnel Sanctions Policy
• System and Information Integrity a list of active agency subscriptions (e.g., CISA, MS-ISAC, US-CERT)

○ Yes
○ No

Primary question answered Yes

1. Did the auditor confirm receipt of all supporting documentation required for the audit?

○ Yes
○ No