U.S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Noncriminal Justice Information Technology Security Audit Policy Reference Guide

Telephone – (304) 625-3020
E-mail – acjis@leo.gov

Revised 10/01/2019

Table of Contents

System Administration

CJIS Systems Officer (CSO)/Repository Manager

The CSO is an individual located within the CSA responsible for the administration of the CJIS network for the CSA. Pursuant to the Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced. The CSO may delegate responsibilities to subordinate agencies. The CSO shall set, maintain, and enforce the following:

1. Standards for the selection, supervision, and separation of personnel who have access to CJI.
2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJI, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.
    a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.
    b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.
    c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.
    d. Ensure the designation of a Terminal Agency Coordinator (TAC) within each agency with devices accessing CJIS systems.
    e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).
    f. Ensure each LASO receives enhanced security awareness training (ref. Section 5.2).
    g. Approve access to FBI CJIS systems.
    h. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.
    i. Perform other related duties outlined by the user agreements with the FBI CJIS Division.
3. Outsourcing of Criminal Justice Functions
    a. Responsibility for the management of the approved security requirements shall remain with the CJA. Security control includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit CJI; and to guarantee the priority service needed by the criminal justice community.
    b. Responsibility for the management control of network security shall remain with the CJA. Management control of network security includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of circuits and network equipment used to transmit CJI; and to guarantee the priority service as determined by the criminal justice community.

(*CJIS Security Policy*, Version 5.7, August 2018, 3 Roles and Responsibilities, 3.2 Roles and Responsibilities for Agencies and Parties, 3.2.2 CJIS Systems Officer [CSO], pp. 5-6.)

The State Identification Bureau (SIB) Chief, i.e. Repository Manager or Chief Administrator, is the designated manager of the agency having oversight responsibility for a state's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

(*CJIS Security Policy*, Version 5.7, August 2018, 3 Roles and Responsibilities, 3.2 Roles and Responsibilities for Agencies and Parties, 3.2.11 Repository Manager, p. 9.)

Information Security Officer (ISO)

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.
2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

(*CJIS Security Policy*, Version 5.8, June 2019, 3 Roles and Responsibilities, 3.2 Roles and Responsibilities for Agencies and Parties, 3.2.8 CJIS System Agency Information Security Officer [CSA ISO], pp. 7-8.)

The CSA ISO shall:

1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
6. Act as a single POC for their jurisdictional area for requesting incident response assistance.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, 5.3.1 Reporting Information Security Events, 5.3.1.1 Reporting Structure and Responsibilities, 5.3.1.1.2 CSA ISO Responsibilities, pp. 23-24.)

Local Agency Security Officer (LASO)

Each LASO shall:

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

(*CJIS Security Policy*, Version 5.8, June 2019, 3 Roles and Responsibilities, 3.2 Roles and Responsibilities for Agencies and Parties, 3.2.9 Local Agency Security Officer [LASO], p. 8.)

Administration of Noncriminal Justice Functions

Agency User Agreements

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (public) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (private) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. An example of a NCJA (private) is a local bank.

All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see Appendix J for supplemental guidance). Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.
(*CJIS Security Policy*, Version 5.7, August 2018, 5 Policy and Implementation, 5.1 Policy Area 1: Information Exchange Agreements, 5.1.1 Information Exchange, 5.1.1.6 Agency User Agreements, p. 17.)

Contracted Noncriminal Justice Services

Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing.

Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.
(*CJIS Security Policy*, Version 5.7, August 2018, 5 Policy and Implementation, 5.1 Policy Area 1: Information Exchange Agreements, 5.1.1 Information Exchange, 5.1.1.8 Outsourcing Standards for Channelers, pp. 17-18.)

Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-

Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.
(*CJIS Security Policy*, Version 5.7, August 2018, 5 Policy and Implementation, 5.1 Policy Area 1: Information Exchange Agreements, 5.1.1 Information Exchange, 5.1.1.8 Outsourcing Standards for Non-Channelers, p. 18.)

Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator2 or (2) the FBI Compact Officer3; and (b) provide the State Compact Officer/Chief Administrator or the FBI Compact Officer copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested.
(Security and Management Control Outsourcing Standard for Non-Channelers, May 2014, 2.0 Responsibilities of the Authorized Recipient, 2.01, p. 4.)

The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.
(*Security and Management Control Outsourcing Standard for Non-Channelers*, May 2014, 2.0 Responsibilities of the Authorized Recipient, 2.02, p. 4.)

The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.
(*Security and Management Control Outsourcing Standard for Non-Channelers*, May 2014, 6.0 Personnel Security, 6.02, p. 9.)

Information Protection

IT Security Program

The *CJIS Security Policy* may be used as the sole security policy for the agency. The local agency may complement the *CJIS Security Policy* with a local policy, or the agency may develop their own stand-alone security policy; however, the *CJIS Security Policy* shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the *CJIS Security Policy* standards.

The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the *CJIS Security Policy* and, where applicable, the local security policy. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. Procedures developed for *CJIS Security Policy* areas can be developed for the security program in general, and for a particular information system, when required.

This document is a compendium of applicable policies in providing guidance on the minimum security controls and requirements needed to access FBI CJIS information and services. These policies include presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions. State, local, and Tribal CJA may implement more stringent policies and requirements. Appendix I contains the references while Appendix E lists the security forums and organizational entities referenced in this document.
(*CJIS Security Policy*, Version 5.8, June 2019, 1 Introduction, 1.3 Relationship to Local Security Policy and Other Policies, pp. 1-2.)

Standards of Discipline

The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.12 Policy Area 12: Personnel Security, 5.12.4 Personnel Sanctions, p. 64.)

Personnel Security

1. To verify identification, state of residency and national fingerprint-based record checks shall be conducted prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing). However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:
    a. 5 CFR 731.106; and/or
    b. Office of Personnel Management policy, regulations, and guidance; and/or
    c. agency policy, regulations, and guidance.

    Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

    See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.
2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.

3. If a record of any kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.
    a. If a felony conviction of any kind exists, the Interface Agency shall deny access to CJI. However, the Interface Agency may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.
    b. Applicants with a record of misdemeanor offense(s) may be granted access if the CSO, or his or her designee, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The Interface Agency may request the CSO review a denial of access determination. This same procedure applies if the person is found to be a fugitive or has an arrest history without conviction.
    c. If a record of any kind is found on a contractor, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the contractor's security officer.
4. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.
5. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI. For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.
6. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
7. The granting agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.12 Policy Area 12: Personnel Security, 5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI, pp. 63-64.)

Upon termination of personnel by an interface agency, the agency shall immediately terminate access to local agency systems with access to CJI. Furthermore, the interface agency shall provide notification or other action to ensure access to state and other agency systems is terminated. If the employee is an employee of a NCJA or a Contractor, the employer shall notify all Interface Agencies that may be affected by the personnel change.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.12 Policy Area 12: Personnel Security, 5.12.2 Personnel Termination, p. 64.)

The agency shall review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.12 Policy Area 12: Personnel Security, 5.12.3 Personnel Transfer, p. 64.)

If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract. (*Security and Management Control Outsourcing Standard for Non-Channelers*, May 2014, 6.0 Personnel Security, 6.01, p. 8.)

Security Awareness Training

Security training is key to the human element of information security. All users with authorized access to CJI should be made aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI. LASOs require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.2 Policy Area 2: Security Awareness Training, p. 20.)

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location. The CSO/SIB Chief may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.2 Policy Area 2: Security Awareness Training, 5.2.1 Awareness Topics, p. 20.)

At a minimum, the following topics shall be addressed as baseline security awareness training for all personnel who have unescorted access to a physically secure location:

1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals.
2. Implications of noncompliance.
3. Incident response (Identify points of contact and individual actions).
4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.2 Policy Area 2: Security Awareness Training, 5.2.1 Awareness Topics, 5.2.1.1 Level One Security Awareness Training, p. 20.)

In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

1. Media protection.
2. Protect information subject to confidentiality concerns — hardcopy through destruction.
3. Proper handling and marking of CJI.
4. Threats, vulnerabilities, and risks associated with handling of CJI.

5. Social engineering.
6. Dissemination and destruction.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.2 Policy Area 2: Security Awareness Training, 5.2.1 Awareness Topics, 5.2.1.2 Level Two Security Awareness Training, p. 20.)

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJI:

1. Rules that describe responsibilities and expected behavior with regard to information system usage.
2. Password usage and management—including creation, frequency of changes, and protection.
3. Protection from viruses, worms, Trojan horses, and other malicious code.
4. Unknown e-mail/attachments.
5. Web usage—allowed versus prohibited; monitoring of user activity.
6. Spam.
7. Physical Security—increases in risks to systems and data.
8. Handheld device security issues—address both physical and wireless security issues.
9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
10. Laptop security—address both physical and information security issues.
11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
12. Access control issues—address least privilege and separation of duties.
13. Individual accountability—explain what this means in the agency.
14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
15. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.
16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.2 Policy Area 2: Security Awareness Training, 5.2.1 Awareness Topics, 5.2.1.3 Level Three Security Awareness Training, p. 21.)

In addition to 5.2.1.1, 5.2.1.2, and 5.1.2.3 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
2. Data backup and storage—centralized or decentralized approach.
3. Timely application of system patches—part of configuration management.
4. Access control measures.
5. Network infrastructure protection measures.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.2 Policy Area 2: Security Awareness Training, 5.2.1 Awareness Topics, 5.2.1.4 Level Four Security Awareness Training, pp. 21-22.)

LASO training shall be required prior to assuming duties but no later than six months after initial assignment, and annually thereafter.

At a minimum, the following topics shall be addressed as enhanced security awareness training for a LASO:

1. The roles and responsibilities listed in *CJIS Security Policy* Section 3.2.9.
2. Additional state/local/tribal/federal agency LASO roles and responsibilities.
3. Summary of audit findings from previous state audits of local agencies.
4. Findings from the last FBI CJIS Division audit of the CSA.
5. Most recent changes to the *CJIS Security Policy*.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.2 Policy Area 2: Security Awareness Training, 5.2.2 LASO Training, p. 22.)

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CSO/SIB Chief/Compact Officer. Maintenance of training records can be delegated to the local level.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.2 Policy Area 2: Security Awareness Training, 5.2.2 Security Training Records, p. 22.)

Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access to CHRI.
(*Security and Management Control Outsourcing Standard for Non-Channelers*, May 2014, 3.0 Responsibilities of the Contractor, 3.04, p. 7.)

Physical Security

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, p. 51.)

A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof.

Sections 5.9.1.1 – 5.9.1.8 describe the physical controls required in order to be considered a physically secure location, while Sections 5.2 and 5.12, respectively, describe the minimum security awareness training and personnel security controls required for unescorted access to a physically secure location. Sections 5.5, 5.6.2.2.1, and 5.10 describe the requirements for

technical security controls required to access CJI from within the perimeter of a physically secure location without AA.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, p. 51.)

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, 5.9.1.1 Security Perimeter, p. 51.)

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, 5.9.1.2 Physical Access Authorizations, p. 51.)

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, 5.9.1.3 Physical Access Control, p. 51.)

The agency shall control physical access to information system distribution and transmission lines within the physically secure location.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, 5.9.1.4 Access Control for Transmission Medium, p. 51.)

The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, 5.9.1.5 Access Control for Display Medium, p. 51.)

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, 5.9.1.6 Monitoring Physical Access, p. 52.)

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, 5.9.1.7 Visitor Control, p. 52.)

The agency shall authorize and control information system-related items entering and exiting the physically secure location.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, 5.9.1.8 Delivery and Removal, p. 52.)

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
2. Lock the area, room, or storage container when unattended.
3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
4. Follow the encryption requirements found in Section 5.10.1.2 for electronic storage (i.e. data "at rest") of CJI.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.2 Controlled Area, p. 52.)

Security Audits

Each CSA shall:

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

Note: This authority does not apply to the audit requirement outlined in the Security and Management Control Outsourcing Standard for Non-Channeler and Channelers related to outsourcing noncriminal justice administrative functions.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.11 Policy Area 11: Formal Audits, 5.11.2 Audits by the CSA, p. 61.)

Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) request and receive written permission from (1) the State Compact Officer/Chief Administrator[2] or (2) the FBI Compact Officer[3]; and (b) provide the State Compact Officer/Chief Administrator or the FBI Compact Officer copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested.

[2] The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contactors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the data the Contactor first receives

CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.
(*Security and Management Control Outsourcing Standard for Non-Channelers*, May 2014, 2.0 Responsibilities of the Authorized Recipient, 2.01 footnote 2, p. 4.)

The Authorized Recipient is responsible for the actions of the Contactor and shall monitor the Contactor's compliance to the terms and conditions of the Outsourcing Standard. For approvals granted through the FBI Compact Officer, the Authorized Recipient shall certify to the FBI Compact Officer that an audit was conducted with the Contactor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement. For approvals granted through the State Compact Officer/Chief Administrator, will conduct an audit of the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement. The Authorized Recipient shall certify to the State Compact Officer/Chief Administrator that the audit was conducted.
(*Security and Management Control Outsourcing Standard for Non-Channelers*, May 2014, 2.0 Responsibilities of the Authorized Recipient, 2.05, p. 5.)

Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.8 Policy Area 8: Media Protection, p. 49.)

The agency shall securely store digital and physical media within physically secure locations or controlled areas. The agency shall restrict access to digital and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.8 Policy Area 8: Media Protection, 5.8.1 Media Storage and Access, p. 49.)

Media Transport

The agency shall protect and control digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.8 Policy Area 8: Media Protection, 5.8.2 Media Transport, p. 49.)

Controls shall be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute physical controls to ensure the security of the data.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.8 Policy Area 8: Media Protection, 5.8.2 Media Transport, 5.8.2.1 Digital Media during Transit, p. 49.)

The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.8 Policy Area 8: Media Protection, 5.8.2 Media Transport, 5.8.2.2 Physical Media in Transit, p. 49.)

Media Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.8 Policy Area 8: Media Protection, 5.8.3 Digital Media Sanitization and Disposal, p. 49.)

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.8 Policy Area 8: Media Protection, 5.8.4 Disposal of Physical Media, p. 49.)

Network Infrastructure

Network Configuration

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams.
The network topological drawing shall include the following:

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

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.7 Policy Area 7: Configuration Management, 5.7.1 Access Restrictions for Changes, 5.7.1.2 Network Diagram, p. 48.)

The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.7 Policy Area 7: Configuration Management, 5.7.2 Security of Configuration Documentation, p. 48.)

Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices.

This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.6.1 Personally Owned Information Systems, p. 33.)

Publicly Accessible Computers

Publicly accessible computers shall not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.6.2 Publicly Accessible Computers, p. 33.)

System Use Notification

The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

1. The user is accessing a restricted information system.
2. System usage may be monitored, recorded, and subject to audit.
3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
4. Use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems:

1. the system use information is available and when appropriate, is displayed before granting access;
2. any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and
3. the notice given to public users of the information system includes a description of the authorized uses of the system.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.4 System Use Notification, p. 32.)

Identification/UserID

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts *at least annually* and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

The agency responsible for account creation shall be notified when:

1. A user's information system usage or need-to-know or need-to-share changes.
2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.1 Account Management, p. 30.)

The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.

Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.2 Access Enforcement, 5.5.2.1 Least Privilege, p. 31.)

Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.1 Identification Policy and Procedures, p. 35.)

In order to manage user identifiers, agencies shall:
1. Uniquely identify each user.
2. Verify the identity of each user.
3. Receive authorization to issue a user identifier from an appropriate agency official.
4. Issue the user identifier to the intended party.
5. Disable the user identifier after a specified period of inactivity.
6. Archive user identifiers.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.3 Identification and Authenticator Management, 5.6.3.1 Identifier Management, p. 41)

Authentication

Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. The CSA/SIB may develop an authentication strategy which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CJI.

Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level. The authentication strategy shall be part of the agency's audit for policy compliance. The FBI CJIS Division shall identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services. The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.2 Authentication Policy and Procedures, pp. 35-36.)

Authenticators are (the something you know, something you are, or something you have) part of the identification and authentication process. Examples of standard authenticators include passwords, hard or soft tokens, biometrics, one-time passwords (OTP) and personal identification numbers (PIN). Users shall not be allowed to use the same password or PIN in the same logon sequence.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.2 Authentication Policy and Procedures, 5.6.2.1 Standard Authenticators, p. 36.)

When agencies use a password as an authenticator for an individual's unique ID, they shall use the basic password standards in 5.6.2.1.1.1, OR follow the advanced password standards in 5.6.2.1.1.2.

NOTE: There is no option to combine or select particular options between the two separate lists below.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.2 Authentication Policy and Procedures, 5.6.2.1 Standard Authenticators, 5.6.2.1.1 Password, p. 36.)

When agencies elect to follow the basic password standards, passwords shall:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the Userid.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.

Not be displayed when entered.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.2 Authentication Policy and Procedures, 5.6.2.1 Standard Authenticators, 5.6.2.1.1.1 Basic Password Standards, p. 36.)

When agencies elect to follow the advanced password standards, follow the guidance below:

1. Passwords shall be a minimum of twenty (20) characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).
2. Password Verifiers shall not permit the use of a stored "hint" for forgotten passwords and/or prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing a password.
3. Verifiers shall maintain a list of "banned passwords" that contains values known to be commonly-used, expected, or compromised. For example, the list may include, but is not limited to:
    a. Passwords obtained from previous breach corpuses
    b. Dictionary words
    c. Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd')
    d. Context-specific words, such as the name of the service, the username, and derivatives thereof

4. When processing requests to establish and change passwords, Verifiers shall compare the prospective passwords against the "banned passwords" list.
5. If the chosen password is found to be part of a "banned passwords" list, the Verifier shall:
    a. Advise the subscriber that they need to select a different password,
    b. Provide the reason for rejection, and
    c. Require the subscriber to choose a different password.
6. Verifiers shall limit the number of failed authentication attempts that can be made as described in Section 5.5.3 Unsuccessful Login Attempts.
7. Verifiers shall force a password change if there is evidence of authenticator compromise or every 365 days from the last password change.
8. Verifiers shall use approved encryption and an authenticated protected channel when requesting passwords to protect against eavesdropping and Man-in-the-Middle (MitM) attacks.
9. Verifiers shall store passwords in a manner that is resistant to offline attacks by salting and hashing the password using a one-way key derivation function when stored.
    a. The salt shall be at least 32 bits in length.
    b. The salt shall be chosen arbitrarily so as to minimize salt value collisions among stored hashes.

    Note: Key derivation functions take a password, a salt, and a cost factor as inputs then generate a password hash. Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive.
10. For each subscriber, Verifiers shall protect stored salt and resulting hash values using a password or PIN.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.2 Authentication Policy and Procedures, 5.6.2.1 Standard Authenticators, 5.6.2.1.1.2 Advanced Password Standards, pp. 36-37.)

In order to manage information system authenticators, agencies shall:
1. Define initial authenticator content.
2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
3. Change default authenticators upon information system installation.
4. Change/refresh authenticators periodically.

Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.3 Identifier and Authenticator Management, 5.6.3.2 Authenticator Management, p. 42.)

Session Lock

The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. 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. Note: an example of a session lock is a screen saver with password.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.5 Session Lock, pp. 32-33.)

Event Logging

Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.

Refer to Section 5.13.6 for additional audit requirements related to mobile devices used to access CJI.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, p. 27.)

The agency's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems.

The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.1 Auditable Event and Content [Information Systems], p. 27.)

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
   a. access permission on a user account, file, directory or other system resource;
   b. create permission on a user account, file, directory or other system resource;
   c. write permission on a user account, file, directory or other system resource;
   d. delete permission on a user account, file, directory or other system resource;
   e. change permission on a user account, file, directory or other system resource.

3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts (i.e. root, Oracle, DBA, admin, etc.).
5. Successful and unsuccessful attempts for users to:
    a. access the audit log file;
    b. modify the audit log file;
    c. destroy the audit log file.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.1 Auditable Event and Content (Information Systems), 5.4.1.1 Events, pp. 27-28.)

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.1 Auditable Event and Content (Information Systems), Events, 5.4.1.1.1 Content, p. 28.)

The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.2 Response to Audit Processing Failures, p. 28.)

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.3 Audit Monitoring, Analysis, and Reporting, p. 28.)

The agency's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.4 Time Stamps, p. 28.)

The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.5 Protection of Audit Information, p. 27.)

The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.6 Audit Record Retention, pp. 28-29.)

A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.7 Logging NCIC and III Transactions, p. 29.)

Advanced Authentication

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates (e.g. public key infrastructure (PKI)), smart cards, software tokens, hardware tokens, paper (inert) tokens, out-of-band authenticators (retrieved via a separate communication service channel – e.g., authenticator is sent on demand via text message, phone call, etc.), or "Risk-based Authentication" that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

When user-based certificates are used for authentication purposes, they shall:

1. Be specific to an individual user and not to a particular device.
2. Prohibit multiple users from utilizing the same certificate.
3. Require the user to "activate" that certificate for each use in some manner (e.g., passphrase or user-specific PIN).

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.2 Authentication Policy and Procedures, 5.6.2.2 Advanced Authentication, pp. 38-39.)

The requirement to use or not use AA is dependent upon the physical, personnel, and technical security controls associated with the user location and whether CJI is accessed directly or indirectly. AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access). Conversely, if the technical security controls have not been met, AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions. The CSO will make the final determination of whether access is considered indirect.

The intent of AA is to meet the standards of two-factor authentication. Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).

EXCEPTION:
AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access. EXAMPLES:

1. A user, irrespective of his/her location, accesses the LEEP portal. The LEEP has AA built into its services and requires AA prior to granting access. AA is required.
2. A user, irrespective of their location, accesses a State's portal through which access to CJI is facilitated. The State Portal has AA built into its processes and requires AA prior to granting access. AA is required.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.2 Authentication Policy and Procedures, 5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale, p. 39.)

When agencies implement the use of a PIN as a standard authenticator, the PIN attributes shall follow the guidance in section 5.6.2.1.1 (password). When agencies utilize a PIN in conjunction with a certificate or a token (e.g. key fob with rolling numbers) for the purpose of advanced authentication, agencies shall follow the PIN attributes described below. For example: A user certificate is installed on a smartphone for the purpose of advanced authentication (AA). As the user invokes that certificate, a PIN meeting the below attributes shall be used to access the certificate for the AA process.

1. Be a minimum of six (6) digits
2. Have no repeating digits (i.e., 112233)
3. Have no sequential patterns (i.e., 123456)
4. Not be the same as the Userid.
5. Expire within a maximum of 365 calendar days.
    a. If a PIN is used to access a soft certificate which is the second factor of authentication, AND the first factor is a password that complies with the requirements in Section 5.6.2.1.1, then the 365 day expiration requirement can be waived by the CSO.
6. Not be identical to the previous three (3) PINs.
7. Not be transmitted in the clear outside the secure location.
8. Not be displayed when entered.

EXCEPTION: When a PIN is used for local device authentication, the only requirement is that it be a minimum of six (6) digits.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.2 Authentication Policy and Procedures, 5.6.2.1 Standard Authenticators, 5.6.2.1.2 Personal Identification Number (PIN), p. 38.)

One-time passwords are considered a “something you have” token for authentication. Examples include bingo cards, hard or soft tokens, and out-of-band tokens (i.e. OTP received via a text message).

When agencies implement the use of an OTP as an authenticator, the OTP shall meet the requirements described below.

1. Be a minimum of six (6) randomly generated characters
2. Be valid for a single session
3. If not used, expire within a maximum of five (5) minutes after issuance

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.2 Authentication Policy and Procedures, 5.6.2.1 Standard Authenticators, 5.6.2.1.3 One-time Passwords (OTP), p. 38.)

Encryption

Encryption is a form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information. Decryption is the reversing of the cryptographic operation to convert the information back into a plaintext (readable) format. There are two main types of encryption: symmetric encryption and asymmetric encryption (also known as public key encryption). Hybrid encryption solutions do exist and use both asymmetric encryption for client/server certificate exchange – session integrity and symmetric encryption for bulk data encryption – data confidentiality.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.1 Information Flow Enforcement, 5.10.1.2 Encryption, p. 54.)

When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.

NOTE: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

EXCEPTIONS:

1. See Sections 5.13.1.2.2 and 5.10.2.
2. Encryption shall not be required if the transmission medium meets all of the following requirements:
    a. The agency owns, operates, manages, or protects the medium.
    b. Medium terminates within physically secure locations at both ends with no interconnections between.
    c. Physical access to the medium is controlled by the agency using the requirements in Sections 5.9.1 and 5.12.
    d. Protection includes safeguards (e.g., acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g., alarms, notifications) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.
    e. With prior approval of the CSO.

Examples:

- A campus is completely owned and controlled by a criminal justice agency (CJA) – If line-of-sight between buildings exists where a cable is buried, encryption is not required.
- A multi-story building is completely owned and controlled by a CJA – If floors are physically secure or cable runs through non-secure areas are protected, encryption is not required.
- A multi-story building is occupied by a mix of CJAs and non-CJAs – If floors are physically secure or cable runs through the non-secure areas are protected, encryption is not required.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.1 Information Flow Enforcement, 5.10.1.2 Encryption, 5.10.1.2.1 Encryption for CJI in Transit, pp. 54-55.)

When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.

1. When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:
   a. Be at least 10 characters
   b. Not be a dictionary word.
   c. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
   d. Be changed when previously authorized personnel no longer require access.
2. Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.

   NOTE: Commonly available encryption tools often use a key to unlock the cipher to allow data access; this key is called a passphrase. While similar to a password, a passphrase is not used for user authentication. Additionally, the passphrase contains stringent character requirements making it more secure and thus providing a higher level of confidence that the passphrase will not be compromised.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.1 Information Flow Enforcement, 5.10.1.2 Encryption, 5.10.1.2.2 Encryption for CJI at Rest, pp. 55.)

For agencies using public key infrastructure (PKI) technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:

1. Include authorization by a supervisor or a responsible official.
2. Be accomplished by a secure process that verifies the identity of the certificate holder.
3. Ensure the certificate is issued to the intended party.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.1 Information Flow Enforcement, 5.10.1.2 Encryption, 5.10.1.2.3 Public Key Infrastructure (PKI) Technology, p. 55.)

Dial-up Access

The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system.

Virtual escorting of privileged functions is permitted only when all the following conditions are met:

1. The session shall be monitored at all times by an authorized escort
2. The escort shall be familiar with the system/area in which the work is being performed.
3. The escort shall have the ability to end the session at any time.
4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
5. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.6 Remote Access, p. 33.)

Mobile Devices

This policy area describes considerations and requirements for mobile devices including smartphones and tablets. Mobile devices are not limited to a single form factor or communications medium. The requirements in this section augment those in other areas of the Policy to address the gaps introduced by using mobile devices.

The agency shall: (i) establish usage restrictions and implementation guidance for mobile devices; and (ii) authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling.
Appendix G provides reference material and additional information on mobile devices.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.13 Policy Area 13: Mobile Devices, p. 66.)

Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery, if so desired by the agency.

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of full featured operating systems may not function properly on devices with limited feature operating systems. MDM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented.

Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time.

Agencies shall implement the following controls when allowing CJI access from devices running a limited-feature operating system:

1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.
2. MDM with centralized administration configured and implemented to perform at least the following controls:
    a. Remote locking of device
    b. Remote wiping of device
    c. Setting and locking device configuration
    d. Detection of "rooted" and "jailbroken" devices
    e. Enforcement of folder or disk level encryption
    f. Application of mandatory policy settings on the device
    g. Detection of unauthorized configurations
    h. Detection of unauthorized software or applications
    i. Ability to determine the location of agency controlled devices
    j. Prevention of unpatched devices from accessing CJI or CJI systems
    k. Automatic device wiping after a specified number of failed access attempts

EXCEPTION: An MDM is not required when receiving CJI from an indirect access information system (i.e. the system provides no capability to conduct transactional activities on state and national repositories, applications or services). However, it is incumbent upon the authorized agency to ensure CJI is delivered to the appropriate requesting agency or individual. The CSO will make the final determination of whether access is considered indirect.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.13 Policy Area 13: Mobile Devices, 5.13.2 Mobile Device Management [MDM], p. 69.)

Organizations shall, at a minimum, ensure that wireless devices:

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

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.13 Policy Area 13: Mobile Devices, 5.13.3 Wireless Device Risk Mitigation, pp. 69-70.)

Certain internal functions on cellular devices may be modified or compromised by the cellular carrier during international use as the devices are intended to have certain parameters configured by the cellular provider which is considered a "trusted" entity by the device.

When devices are authorized to access CJI outside the U.S., agencies shall perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency's policies prior to and after deployment outside of the U.S.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.13 Policy Area 13: Mobile Devices, 5.13.1 Wireless Communication Technologies, 5.13.1.2 Cellular Devices, 5.13.1.2.1 Cellular Service Abroad, p. 68.)

Personal Firewalls

For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems). At a minimum, the personal firewall shall perform the following activities:

1. Manage program access to the Internet.
2. Block unsolicited requests to connect to the user device.
3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

Mobile devices with limited feature operating systems (i.e. tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and to a certain extent, perform functions similar to a personal firewall on a device with a full feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.13 Policy Area 13: Mobile Devices, 5.13.4 System Integrity, 5.13.4.3 Personal Firewall pp. 70-71.)

Bluetooth Access

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth is used primarily to establish wireless personal area networks (WPAN). Bluetooth technology has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, headsets, and biometric capture devices.

Bluetooth technology and associated devices are susceptible to general wireless networking threats (e.g. denial of service [DoS] attacks, eavesdropping, man-in-the-middle [MITM] attacks, message modification, and resource misappropriation) as well as specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency's operational and business processes.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.13 Policy Area 13: Mobile Devices, 5.13.1 Wireless Communications Technologies, 5.13.1.3 Bluetooth, p. 68.)

Wireless (802.11x) Access

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used.

Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:

1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.
2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
5. Enable user authentication and encryption mechanisms for the management interface of the AP.
6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Section 5.6.2.1.
7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.
8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.
10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
11. Ensure that the ad hoc mode has been disabled.
12. Disable all nonessential management protocols on the APs.
13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.
14. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
15. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.13 Policy Area 13: Mobile Devices, 5.13.1 Wireless Communication Technologies, 5.13.1.1 802.11 Wireless Protocols, pp. 66-67.)

Many mobile devices include the capability to function as a WiFi hotspot that allows other devices to connect through the device to the internet over the devices cellular network.

When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they shall be configured:

1. Enable encryption on the hotspot
2. Change the hotspot's default SSID
    a. Ensure the hotspot SSID does not identify the device make/model or agency ownership

3. Create a wireless network password (Pre-shared key)
4. Enable the hotspot's port filtering/blocking features if present
5. Only allow connections from agency controlled devices

Note: Refer to the requirements in Section 5.10.1.2 encryption for item #1. Refer to the requirements in Section 5.6.2.2.1 Password for item #3. Only password attributes #1, #2 and #3 are required.

OR

1. Have a MDM solution to provide the same security as identified in items 1 – 5 above.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.13 Policy Area 13: Mobile Devices, 5.13.1 Wireless Communication Technologies, 5.13.1.4 Mobile Hotspots, pp. 68-69.)

Boundary Protection

The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see Section 5.5) are:

1. Prevent CJI from being transmitted unencrypted across the public network.
2. Block outside traffic that claims to be from within the agency.
3. Do not pass any web requests to the public network that are not from the internal web proxy.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g. proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.1 Information Flow Enforcement, p. 53.)

The agency shall:

1. Control access to networks processing CJI.
2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.13.4.3 for guidance on personal firewalls.
4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device "fails closed" vs. "fails open").
6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in Section 5.10.3.2 to achieve separation.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.1 Information Flow Enforcement, 5.10.1.1 Boundary Protection, pp. 53-54.)

Intrusion Detection Tools and Techniques

Intrusion detection systems are deployed inside a network to monitor events against a known set of parameters (i.e. malicious activity or policy violations) and make notification to the system of any event which violates any of those parameters. They are passive in nature, listening and monitoring network traffic. There are mainly two types of IDS; network-based IDS (NIDS) and host-based IDS (HIDS).

Intrusion prevention systems are an IDS with the capability to respond to detected intrusions. They are normally deployed at the perimeter of a network, scanning traffic. Like detection systems, protection systems compare scanned traffic to defined normal parameters but unlike detection systems are able to take some type of immediate action to mitigate, or prevent, an event.

Agencies shall:

1. Implement network-based and/or host-based intrusion detection or prevention tools.
2. Maintain current intrusion detection or prevention signatures.
3. Monitor inbound and outbound communications for unusual or unauthorized activities.
4. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.
5. Review intrusion detection or prevention logs weekly or implement automated event notification.
6. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.1 Information Flow Enforcement, 5.10.1.3 Intrusion Detection Tools and Techniques, pp. 55-56.)

Malicious Code Protection

The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.4 System and Information Integrity Policy and Procedures, 5.10.4.2 Malicious Code Protection, p. 59.)

Spam and Spyware Protection

The agency shall implement spam and spyware protection.

The agency shall:

1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
2. Employ spyware protection at workstations, servers and mobile computing devices on the network.
3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this Policy.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.4 System and Information Integrity Policy and Procedures, 5.10.4.3 Spam and Spyware Protection, p. 59.)

Security Alerts and Advisories

The agency shall:

1. Receive information system security alerts/advisories on a regular basis.
2. Issue alerts/advisories to appropriate personnel.
3. Document the types of actions to be taken in response to security alerts/advisories.
4. Take appropriate actions in response.
5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.4 System and Information Integrity Policy and Procedures, 5.10.4.4 Security Alerts and Advisories, pp. 59-60.)

Patch Management

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as:

1. Testing of appropriate patches before installation.
2. Rollback capabilities when installing patches, updates, etc.
3. Automatic updates without individual user intervention.
4. Centralized patch management.

Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.4 System and Information Integrity Policy and Procedures, 5.10.4.1 Patch Management, pp. 58-59.)

Based on the varying connection methods for mobile devices, an always on connection cannot be guaranteed for patching and updating. Devices without always-on cellular connections may not be reachable for extended periods of time by the MDM or solution either to report status or initiate patching.

Agencies shall monitor mobile devices to ensure their patch and update state is current.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.13 Policy Area 13: Mobile Devices, 5.13.3 Wireless Device Risk Mitigations, 5.13.4.1 Patching/Updates, p. 70.)

Voice over Internet Protocol (VoIP)

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are lower costs than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol (IP) services. Among VoIP's risks that have to be considered carefully are: myriad security concerns, cost issues associated with new networking hardware requirements, and overarching quality of service (QoS) factors.

In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:

1. Establish usage restrictions and implementation guidance for VoIP technologies.
2. Change the default administrative password on the IP phones and VoIP switches.
3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.

Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.1 Information Flow Enforcement, 5.10.1.4 Voice Over Internet Protocol, p. 56.)

Partitioning and Virtualization

As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization have existed for a while, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.3 Partitioning and Virtualization, p. 57.)

The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.
The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following:

1. Different computers.
2. Different central processing units.
3. Different instances of the operating system.
4. Different network addresses.
5. Other methods approved by the FBI CJIS ISO.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.3 Partitioning and Virtualization, 5.10.3.1 Partitioning, pp. 57-58.)

Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for criminal justice and noncriminal justice activities. In addition to the security controls described in this Policy, the following additional controls shall be implemented in a virtual environment:

1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines (VMs) that process CJI internally or be separated by a virtual firewall.
4. Drivers that serve critical functions shall be stored within the specific VM they service. In other words, do not store these drivers within the hypervisor, or host operating system, for sharing. Each VM is to be treated as an independent system – secured as independently as possible.

The following additional technical security controls shall be applied in virtual environments where CJI is comingled with non-CJI:

1. Encrypt CJI when stored in a virtualized environment where CJI is comingled with non-CJI or segregate and store unencrypted CJI within its own secure VM.
2. Encrypt network traffic within the virtual environment.

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Implement IDS and/or IPS monitoring within the virtual environment.
2. Virtually or physically firewall each VM within the virtual environment to ensure that only allowed protocols will transact.
3. Segregate the administrative duties for the host.

Appendix G-1 provides some reference and additional background information on virtualization.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.3 Partitioning and Virtualization, 5.10.3.2 Virtualization, p. 58.)

Cloud Computing

Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., purported cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center on FBI.gov, NIST Special Publications (800-144, 800-145, and 800-146), as well as the cloud provider's policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.

The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e. U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).

Note: This restriction does not apply to exchanges of CJI with foreign government agencies under international exchange agreements (i.e. the Preventing and Combating Serious Crime (PCSC) agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).

Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.

The agency may permit limited use of metadata derived from unencrypted CJI when specifically approved by the agency and its "intended use" is detailed within the service agreement. Such authorized uses of metadata may include, but are not limited to the following: spam and spyware filtering, data loss prevention, spillage reporting, transaction logs (events and content – similar to Section 5.4), data usage/indexing metrics, and diagnostic/syslog data.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.1 Information Flow Enforcement, 5.10.1.5 Cloud Computing, pp. 56-57.)

Security Incident Response

The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of CJI, agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Appendix F contains a sample incident notification letter for use when communicating the details of a CJI-related incident to the FBI CJIS ISO.

Refer to Section 5.13.5 for additional incident response requirements related to mobile devices used to access CJI.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, p. 24.)

The agency shall promptly report incident information to appropriate authorities. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users

shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, 5.3.1 Reporting Security Events, p. 24.)

The CSA ISO shall:

1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
6. Act as a single POC for their jurisdictional area for requesting incident response assistance.

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, 5.3.1 Reporting Information Security Events, 5.3.1.1 Reporting Structure and Responsibilities, 5.3.1.1.2 CSA ISO Responsibilities, pp. 24-25.)

A consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, 5.3.2 Management of Security Incidents, p. 25.)

The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, 5.3.2 Management of Security Incidents, 5.3.2.1 Incident Handling, p. 25.)

Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, 5.3.2 Management of Security Incidents, 5.3.2.2 Collection of Evidence, p. 25.)

The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, 5.3.3 Incident Response Training, p. 24.)

The agency shall track and document security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.
(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, 5.3.4 Incident Monitoring, p. 25.)

In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.

Special reporting procedures for mobile devices shall apply in any of the following situations:

1. Loss of device control. For example:
    a. Device known to be locked, minimal duration of loss
    b. Device lock state unknown, minimal duration of loss
    c. Device lock state unknown, extended duration of loss
    d. Device known to be unlocked, more than momentary duration of loss
2. Total loss of device
3. Device compromise
4. Device loss or compromise outside the United States

(*CJIS Security Policy*, Version 5.8, June 2019, 5 Policy and Implementation, 5.13 Policy Area 13: Mobile Devices, 5.13.5 Incident Response, p. 71.)

The Authorized Recipient shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference. The Authorized Recipient shall develop and maintain a written incident reporting plan for security events, to include violations and incidents. (See also Sections 2.07 and 3.03)
(*Security and Management Control Outsourcing Standard for Non-Channelers*, May 2014, 8.0 Security Violations, 8.01(a), p. 10)