WISCONSIN

TIME SYSTEM

Training Materials

LOCAL AGENCY SECURITY

OFFICER (LASO)

TRAINING HANDOUT

The Local Agency Security Officer (LASO) is the primary Information Security Officer of the law enforcement agency and should be familiar with the agency's computer and network systems. The LASO should also be familiar with the current version of the CJIS Security Policy, published by the Criminal Justice Information Services (CJIS) Division of the FBI. The CJIS Security Policy sets out the minimum requirements for the protection of criminal justice information.

Purpose

The intent of LASO training is to provide agency LASOs with:

1. An understanding of their required roles & responsibilities,
2. An understanding of what criminal justice information (CJI) is,
3. A summary of recent audit findings by the state and the FBI, and
4. A summary of changes to the CJIS Security Policy.

What is Criminal Justice Information (CJI)?

The primary function of the CJIS Security Policy is to set minimum requirements for the protection of Criminal Justice Information (CJI). But what is CJI? What will you be protecting as the LASO?

Criminal Justice Information is any restricted information obtained from the National Crime Information Center (NCIC). The following are examples of CJI that should be protected:

- Biometric data: data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population (fingerprints, palm prints, iris scans, facial recognition data)
- Property data: information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII)
- Identity history data: textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for identified individuals
- Biographic data: information about individuals associated with a unique case and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case
- Case/incident history data: information about the history of criminal incidents.

LASO Training Requirements

LASO training is required to be completed prior to assuming the duties of the LASO and annually thereafter.

Each LASO shall:

1. Identify who is using the CIB 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 the CJIS Security Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the Wisconsin Information Security Officer is promptly informed of security incidents.

Identify Users

The LASO must know who is using the agency's hardware, software, and firmware and ensure no unauthorized individuals or processes have access.

Agencies must keep a current Authorized User List of all personnel who have unescorted access to the physically secure location, CJIS data (electronic and/or hard copy), and logical (i.e., virtual or remote) access to data, systems, and networks. This can include physical and logical access. This list must be kept current and remove any personnel who no longer need access. Agencies should review and update the Authorized User List at least once a year.

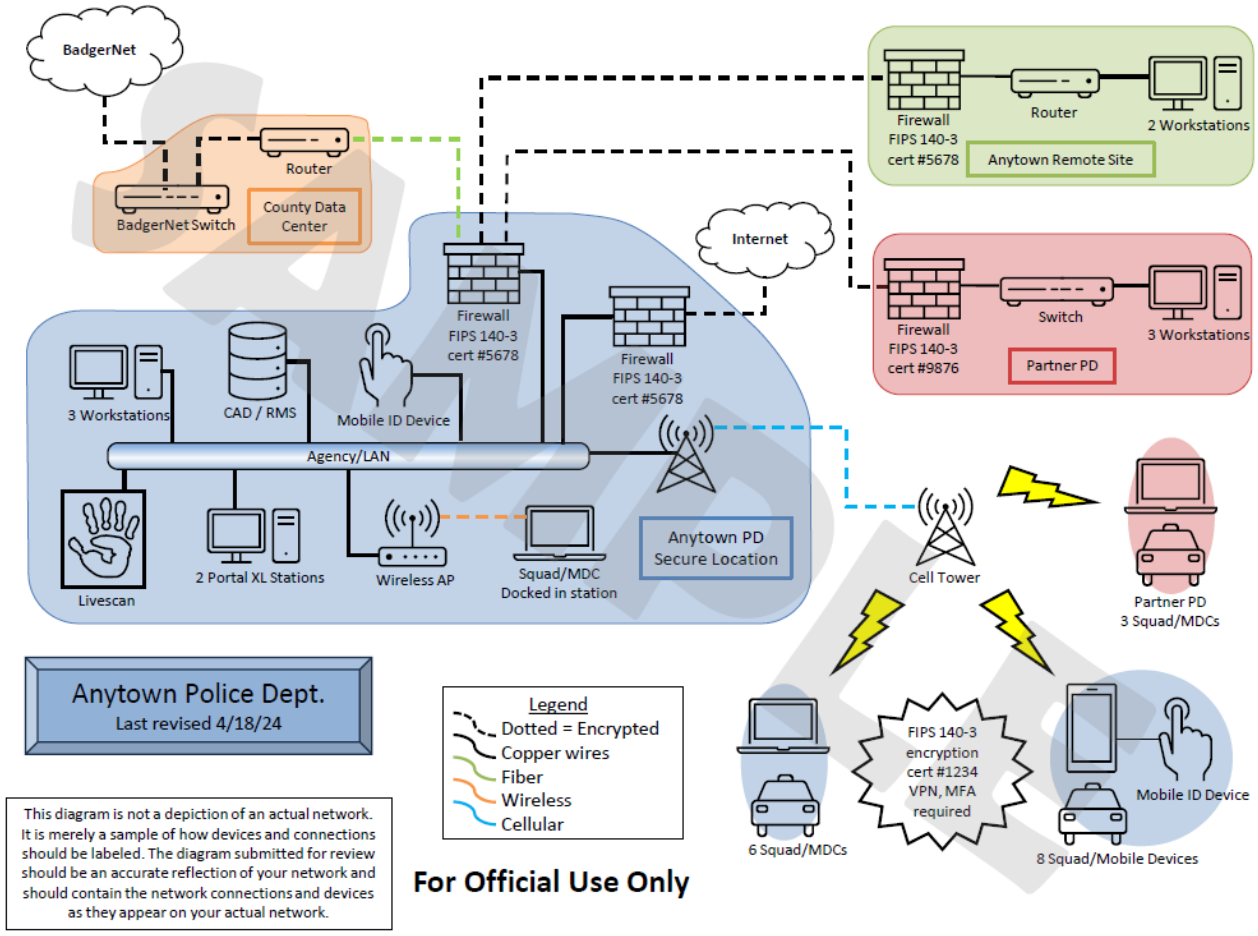
Authorized personnel are users that have passed a fingerprint-based background check, completed Security Awareness training prior to appointment of their position and appear on the agency's authorized user list.

Agencies should keep all hardware and software up-to-date and ensure any encryption meets the CJIS Security Policy requirements.

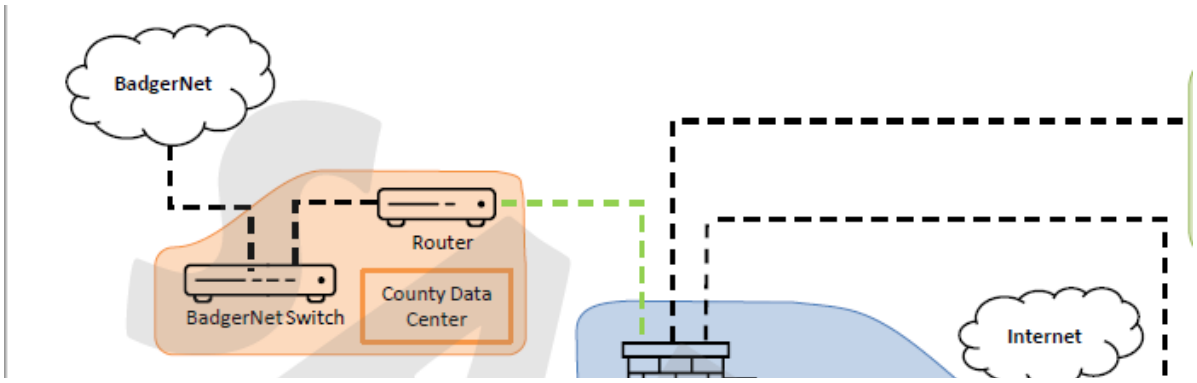
Identify and Document Equipment

The LASO will be responsible for understanding the agency's criminal justice network and its security measures and how it connects to the state system operated by the Crime Information Bureau (CIB).

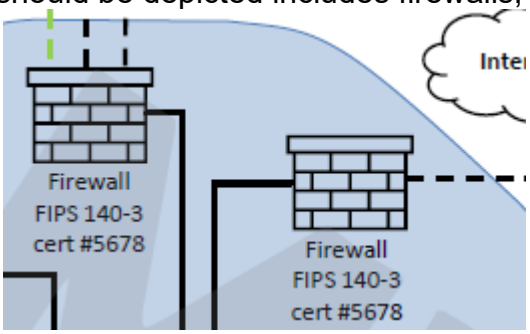
The CJIS Security Policy and CIB require that you maintain a network diagram to display how your agency network is set up and how systems are interconnected. Below is a sample diagram and an explanation of each of the requirements that CIB needs to see within the diagram.



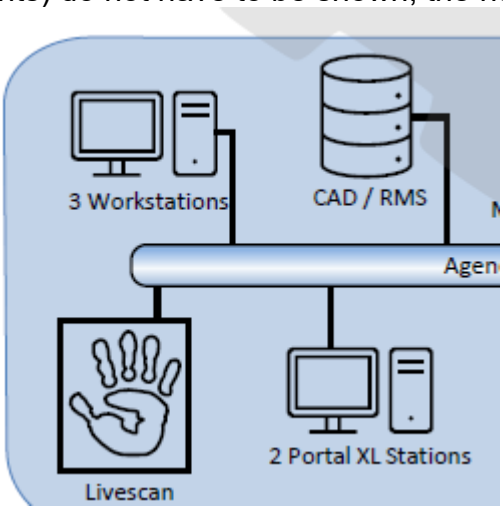
1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the BadgerNet/agency endpoint.



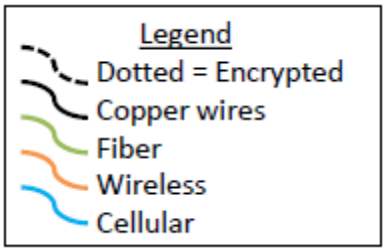
2. Depict all entry points into the network including any hardware components that are used to isolate the network from other networks at the agency (hardware that should be depicted includes firewalls, switches, routers, servers, etc.).



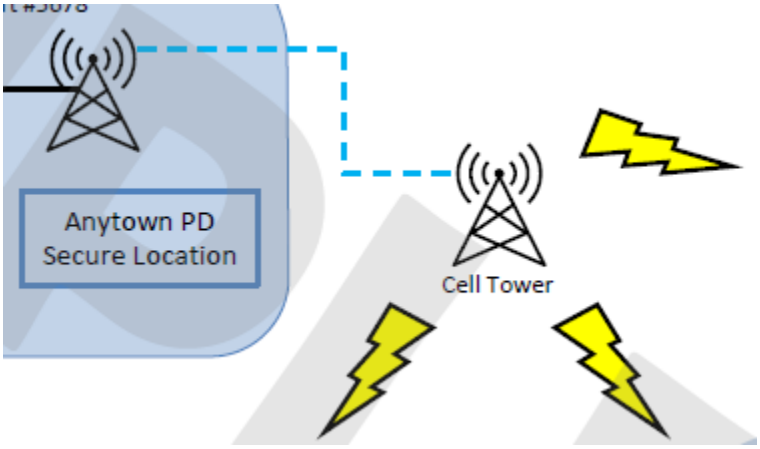
3. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.



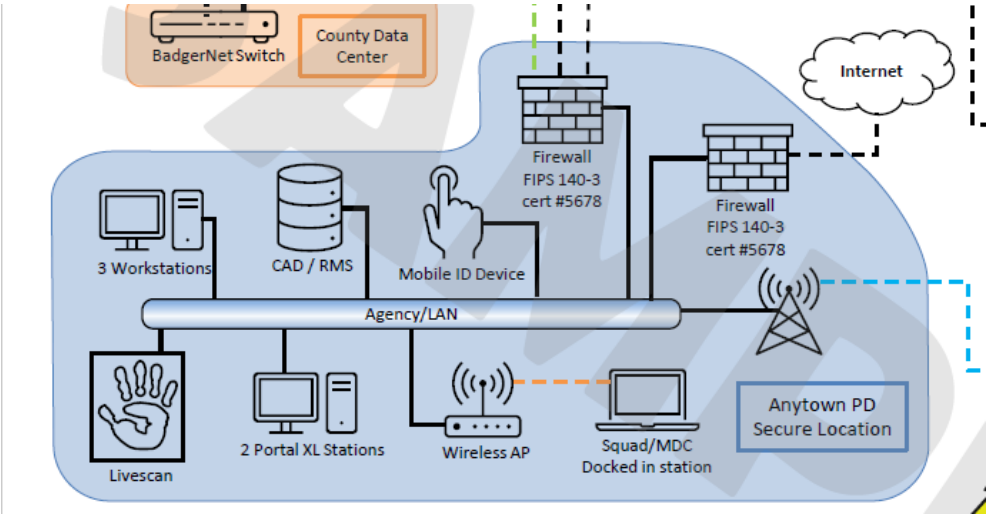
4. Depict the beginning point of data encryption and the point where data is decrypted. Identify each segment of the network through which encrypted data passes. A legend is helpful to differentiate encrypted connections from unencrypted connections. The diagram should have the FIPS certificate number added for corresponding encryption devices and connections.



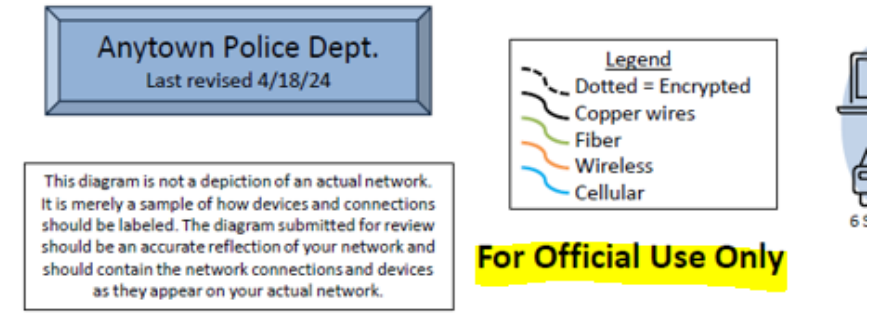
5. Identify the transmission methods (data circuit, microwave, cellular technologies, fiber optics, copper wiring, etc.) being used to transmit or receive TIME/CJIS data.



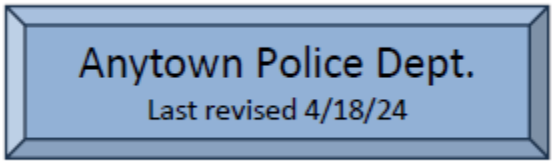
6. Clearly indicate the boundaries of your criminal justice facility in relation to the equipment illustrated on the diagram.



7. "For Official Use Only" (FOUO) markings.



8. The agency name and date (day, month, year) the drawing was created or updated.



Personnel Security

The LASO must ensure personnel security requirements are being met, including the screening of new personnel and users.

Prior to being granted unescorted access to criminal justice information, a new employee, vendor, or contractor is required to pass a fingerprint-based background check. Fingerprints are submitted to the Crime Information Bureau (CIB) and the results of the Wisconsin and III checks are returned to the agency's Wisconsin Online Record Check System (WORCS) account. The administrator for your agency's WORCS account must review the results to determine if access to CJIS data should be allowed. If a felony conviction is identified during the review and the agency feels that access should be granted, they must request a variance from the CSO prior to allowing access.

When a fingerprint-based background check is conducted, the person being printed shall be given a copy of the Privacy Statement and Challenge Notice. The Privacy Statement explains when and how the fingerprints might be used. The Challenge Notice explains that anybody may challenge the results of a fingerprint check and provides information on how to do so.

If your agency uses a Cloud Provider, a fingerprint-based background check may not be required depending on the type of service and who has access to encryption keys. If there is no access to encryption keys by any personnel of the Cloud Provider, a fingerprint-based background check is not needed, as the personnel would not have unescorted access to the CJI.

In addition to the fingerprint submission, a name-based search must be conducted for warrants and if the person is not a Wisconsin resident, a search of the out-of-state's criminal history repository must also be submitted.

Security Measures

As the LASO, you are responsible for ensuring the security of the agency, both physical and logical. Here are some ways to ensure physical security:

- Physically secured areas should be posted with signs indicating "Authorized Personnel Only" at all entrances.
- Have a policy for identifying individuals within the secured area and prior to allowing someone access to your secured area.
- Visitors and unauthorized personnel must be escorted at all times by an authorized person.
- CJIS information should be protected from viewing by unauthorized personnel by using screen protectors, locking computers when personnel leave their workstation, keeping TIME System printouts out of sight of visitors.

Policy Compliance

Agency policy should be guided by the most current version of the CJIS Security Policy. Agencies are required to meet the minimum standards laid out in the policy. All agencies with TIME System access will be audited by the Crime Information Bureau (CIB) to ensure compliance.

In your role as LASO, you will be involved in the audit and be responsible for answering questions regarding the agency's technical security.

One very important role of the LASO is to inform CIB of any security incident. A security incident can include malicious code, ransomware, a phishing attack, or social engineering, to name a few. As the LASO, you will be required to liaise with CIB during the process of cleaning up and reinstating TIME System access at your agency.

You should inform CIB immediately if there is a security incident (or potential security incident) by emailing tscc@wisdoj.gov. or call TIME System Control Center (TSCC) at (608) 266-7633.

State and National Audit Findings

Just as every agency with TIME System access in Wisconsin is audited by CIB once in a three-year cycle, the State of Wisconsin is also audited by the FBI. Below are some of the findings based on the most recent national audit by the FBI and the state audits of Wisconsin agencies.

The CIB audit will generally include two questionnaires: a TIME System questionnaire, which will focus on policy, procedure, training, quality assurance, and records review, and a Technical Security questionnaire, which will focus on the technical requirements of the CJIS Security Policy including network design, access, controls, and protections.

The findings below are common items that were identified during the past state audit cycle as out of compliance with the CJIS Security Policy. The LASO should ensure that each of these items are compliant within their own agency.

Many agencies fail to perform the necessary fingerprint-based background checks. Sworn officers and jailers are required to have fingerprints submitted to Training and Standards for the DOJ-LE 303 form, but this does not meet the requirements for the CJIS Security Policy. Sworn officers and jailers should have two sets of prints taken, one for Training and Standards, and one for the Crime Information Bureau (CIB). Civilian personnel, vendors, and contractors must have one set of fingerprints submitted to CIB. Once these prints are submitted, CIB will run them through the Wisconsin Criminal History Repository and forward them to the FBI. All results will be returned to the agency's Wisconsin Online Record Check System (WORCS) account for review. A review of the results must take place before unescorted access can be granted. Agencies should have at least one person designated as the WORCS administrator, with the capability to log in to WORCS and pull the results from the site for review.

All agencies that access the TIME System or store Criminal Justice Information (CJI) are required to have a security incident response policy. Each year we ask if agencies have a policy in place and agencies often respond "no". Agencies are required to have this policy in effect in their agency, and all personnel, contractors, and vendors are required to know the policy and to whom they should report any suspicious activity. The security incident response policy should include elements such as adequate preparation, detection, analysis, containment, recovery, and user response activities. Agencies are also required to track, document, and report incidents to CIB.

Updates to the CJIS security policy require that all devices which can access, transmit or process CJI must have Multi Factor Authentication (MFA) deployed regardless of location. There are multiple solutions available to meet this requirement. The requirement for MFA is sanctionable now.

Another area where agencies are not compliant with the requirements of the CJIS Security Policy are intrusion detection/prevention systems (IDS/IPS) and their requirements. All agencies are required to have network-based or host-based intrusion detection or prevention tools deployed on their network where CJI is accessed, processed, transmitted, or stored. Agencies must also maintain current intrusion detection or prevention signatures, monitor inbound and outbound communications for unusual or unauthorized activities, and employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks. Agencies must send intrusion detection logs to a central logging facility where correlation and analysis can take place. This can be to a Security Incident Event Management (SIEM) or other software/product that can analyze the logs, not necessarily sent out to a third party. Agencies must review intrusion detection or prevention logs weekly or implement automated event notification.

Many agencies were found to be out of compliance with encryption of CJI. When CJI is transmitted electronically, the current CJISSECPOL requires it must be encrypted with a FIPS 140-3 certified encryption module or FIPS validated, 128-bit AES algorithm if the CJI leaves the physically secure location. If your agency currently has encryption, you should reach out to IT Support or device/application vendor and ask for the FIPS 140-3

certificate that covers the encryption module or FIPS certified algorithm. Agencies utilizing current FIPS 140-2 encryption will be compliant until September 21st, 2026. Starting October 1st, 2026, the minimum requirement for encryption will be FIPS 140-3 certified encryption modules or FIPS validated algorithm for symmetric key encryption and decryption (FIPS 197 [AES]), with a symmetric cipher key of at least 128-bit strength for CJI in-transit.

Many agencies do not have a LASO assigned or their LASO has not completed the required annual training through TRAIN. An agency's LASO is required to complete LASO training prior to appointment and annual thereafter. Currently, LASO training is available via online module or by printing it out from WILENET. The handout is available at https://wilenet.widoj.gov/cib/time-system-training-materials-manuals-forms.

State auditors have found that agencies do not have a network diagram, or the network diagram does not include all required information. Network diagrams are missing the name of agency, date of creation, or "For Official Use Only" markings. Diagrams are also missing key pieces of infrastructure including labeled firewalls, servers, virtual environment, wireless access points, or FIPS certificates added to corresponding encryption devices and connections.

Review of records entered by Wisconsin agencies identify that records are not entered using all available data, including data from CHRI, DOT, DNR, DOC, and in-house records. Agencies were also found to not be contacting the court or complainant to ensure the entry is still valid (warrant is still outstanding, missing person still missing, property still missing/stolen, etc.).

Wisconsin was last audited by the FBI in 2025 and will be audited again in 2028. There were several findings on the 2025 audit for Information Technology (ITS) and NCIC categories. Findings on the ITS audit include:

- Agencies are not ensuring they have required policies and procedures in place and documented for the following controls: Awareness and Training (AT), Auditing and Accountability (AU), Access Control (AC), Identification and Authentication (IA), Physical and Environmental Protection (PE), Mobile Devices, System and Information Integrity (SI).
- Agencies do not have media disposal requirements documented and implemented.
- Agencies do not have the required system use notification message displayed prior to accessing CJI.
- Agencies are not ensuring audit and accountability controls are implemented on information systems accessing CJI. Agencies are not reviewing system audit logs at least weekly for inappropriate, unusual, or suspicious activity.
- Agencies are not ensuring that Multi-Factor Authentication (MFA) is implemented for access to CJI.
- Agencies are not ensuring CJI transmitted or stored outside the boundary of the physically secure location is protected via encryption.

- Agencies do not have a security incident response policy documented and implemented.

From the 2025 NCIC audit of Wisconsin, there were three findings:

- Agencies are not placing Locates on corresponding NCIC records after hit confirmation.
- Agencies are not ensuring NCIC records contain all available information.
- Agencies are not ensuring the use and dissemination of Interstate Identification Index (III) information is authorized.

Changes to the CJIS Security Policy

The FBI started a multi-year revamp of the CJIS Security Policy in 2022. Over the past few years, each section of the policy has been updated. The most recent version (6.0) was released December 27, 2024.

Version 5.9.5 added priorities and implementation markings denoting sanctionable dates to the CJIS Security Policy Companion Document. Policy sections which have not been modernized and priority one controls are currently sanctionable. Modernized controls published prior to the release of v5.9.5 may fall into existing priority two, three and four levels and are sanctionable by end of year 2025, 2026, and 2027 respectively. Those modernized controls that are considered to fall under the "Zero Cycle" are being asked about to educate agencies on coming requirements that will be sanctionable for audit as of October 1, 2027. The Zero Cycle began October 1, 2024, and ends September 30, 2027. Non-existing controls marked priority two, three or four are marked as Zero-cycle items and are annotated with an asterisk. Below are some of the recent updates to the CJIS Security Policy.

5.9.3 Updates

MP-1 Policies and Procedures: Agencies are already required to have policies relating to media protection. The update requires that agencies develop procedures to facilitate the implementation of the media protection policy and the associated media protection controls. An individual with security responsibilities must be designated to manage the development, documentation, and dissemination of the media protection policies and procedures. These policies and procedures are to be reviewed and updated at least annually and following any security incidents involving digital and/or non-digital media.

MP-2 Media Access: Agencies will continue to restrict access to digital and non-digital media to authorized individuals. An Authorized User is someone who has passed a fingerprint-based background check, completed Security Awareness Training, and appears on your agency's Authorized User List.

MP-4 Media Storage: Agencies will continue to physically control and securely store digital and non-digital media within the physically secure locations or controlled areas and encrypt CJI on digital media when physical and personnel restrictions are not

*Sanctionable for audit beginning October 1, 2027

feasible. Agencies will also protect system media types where CJI is encrypted on digital media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

MP-5 Media Transport: Agencies will continue to protect and control digital and non-digital media to help prevent compromise of the data during transport outside of the physically secure location or controlled areas. Physical media will be protected at the same level as the information would be protected in electronic form. Agencies will restrict the activities associated with transport of electronic and physical media to authorized personnel. A new requirement with this update is that agencies will maintain accountability for system media during transport outside the physically secure location or controlled areas and document activities associated with the transport of system media. Agencies will continue to restrict activities associated with the transport of system media to authorized personnel only.

MP-6 Media Sanitization: Agencies will continue to sanitize or destroy digital and non-digital media prior to disposal, release from agency control, or release for reuse using an overwrite technology at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable media will be destroyed, and physical media will be securely disposed of when no longer needed for investigative or security purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration. Agencies will need to employ sanitization mechanisms with strength and integrity commensurate with the security category or classification of the information.

MP-7 Media Use: A new requirement with this update, agencies will restrict the use of digital and non-digital media on agency owned systems that store, process, transmit CJI by using technical, physical, or administrative controls. Agencies will prohibit the use of personally owned digital media devices on all agency owned or controlled systems that store, process, or transmit CJI. Agencies will prohibit the use of digital media devices on all agency owned or controlled systems that store, process, or transmit CJI when such devices have no identifiable owner.

AT-1* Awareness and training policies and procedures: This update to the policy requires each agency to have an awareness and training policy and procedures. This policy must be disseminated to all personnel with unescorted logical or physical access to CJI. These policies and procedures must be reviewed / updated annually and after a security incident occurs.

AT-3(5) * Role based training – processing personally identifiable information (PII): Provide at initial employment and annually personally identifiable information training to all personnel with unescorted logical or physical access to CJI.

IR-1 Incident response policy and procedures: Updates to the Incident response policy and procedures require that the agency's incident response policy and procedures are reviewed / updated annually and after a security incident occurs.

*Sanctionable for audit beginning October 1, 2027

IR-2(3) * Incident response training: Provide incident response training to agency personnel consistent with a user's assigned roles and responsibilities (to include the process for reporting a breach). Review and update the incident response training content annually.

IR-3* Incident response testing: Each agency must test the effectiveness of their incident response procedures with tabletop or walkthrough exercises, simulation, or other agency appropriate testing. Coordinate incident response testing with personnel responsible for related plans.

IR-8(1) * Incident response plan / breaches: Incident response plans must include a provision to determine if individuals or other organizations (including oversight organizations) need to be notified as a result a PII data breach. The incident response plan must include an assessment to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and mechanisms to mitigate such harms. The incident response plan must also identify applicable privacy requirements.

AC-1* Access control policy and procedures: This update to the policy requires each agency to have an access control policy and procedures. This policy must be disseminated to all personnel with access control responsibilities. These policies and procedures must be reviewed / updated annually and after a security incident occurs.

AC-2 Account management: Updates to this section of the policy require agencies to list access authorizations and attributes for each account (e.g. email, employer ORI, state sworn officer indicator etc.). This section of policy also requires account managers and/or system administrators to be notified within one day when a user is terminated/transferred, when the account is no longer required or when system usage or need to know changes for an individual. Support the management of system accounts by using automated mechanisms. AC-2 also sets timetables for accounts be disabled under circumstances such as account expiration, inactive accounts, violation of organizational policy, etc. Users are required to log out at the end of their work period.

AC-7 Unsuccessful logon attempts: Updates to section AC-7 define the number of unsuccessful log-on attempts before an account must be locked. Enforce a limit of five (5) consecutive invalid logon attempts by a user during a 15-minute period.

AC-12* Session termination: This new requirement requires that a user's session is automatically terminated when a user has been logged out.

AC-14* Permitted actions without identification/ authentication: Agencies shall determine actions that can be performed without identification or authentication. Document and provide rationale in the security plan for actions which do not require identification/authentication.

AC-20 Use of external systems: Updates to section AC-20 prohibit the use of personally owned information systems (including mobile devices) and publicly

*Sanctionable for audit beginning October 1, 2027

accessible system for accessing, processing, storing, or transmitting CJI.

AC-22* Publicly accessible content: Designate and train individuals to make information publicly accessible. Review proposed content of information prior to posting content to publicly accessible system. Review content on a quarterly basis to ensure that non-public information has not been released and remove if discovered.

IA-1* Identification and authentication policy and procedures: This update to the policy requires each agency to have an identification and authentication policy and procedures. This policy must be disseminated to all personnel with unescorted access to CJI. These policies and procedures must be reviewed / updated annually and after a security incident occurs. Sample policies are available on WILENET.

IA-2 Identification and authentication of organizational users: Deploy multifactor authentication (MFA) for all user accounts with access to networks or systems which transmit, process, store CJI. MFA must be replay resistant.

IA-3* Device identification and authentication: Uniquely identify and authenticate devices before establishing remote or network connections. In the case of local connection, the device must be approved by the agency and identified prior to connection to agency assets.

IA-4 Identifier management: New requirements of IA-4 include preventing the reuse of identifiers for one (1) year and identifying each individual as agency or non-agency.

IA-5 Authenticator management: The updates to authenticator management section of policy included requirements for specific authenticators (See IA-5(1)), controls to protect authenticators from unauthorized access/ loss and requirement to ensure that the authenticator is associated with authorized personnel**.** Consult your IT service provider to determine which authenticators will work best with your agency's system.

IA-7* cryptographic module authentication: Implement mechanisms for authentication before granting access to cryptographic modules that meet executive orders, directive, policies, regulations, standards, and guidelines for such authentication.

IA-8* Identification and authentication (non-organization users): Uniquely identify and authenticate non-organizational users or processes acting on their behalf. Ensure that only NIST compliant external authenticators are accepted by your agency and maintain a list of accepted external authenticators. Conform to Security Assertation Markup Language (SAML) or Open ID Connect (OIDC) identity management profiles.

IA-11* Re-authentication: Require users to re-authenticate when roles, authenticators, or credentials change, when privileged functions are executed or every 12 hours. (12 hours is the maximum amount of time and there are no exceptions to that.)

*Sanctionable for audit beginning October 1, 2027

IA-12* Identity proofing: This section of policy covers identity proofing of system users. The identity proofing process resolves a user's identity to a unique individual by collecting, validating, and verifying identity evidence. Identity proofing procedures must include redress mechanism for issues that may arise from identity proofing. Information regarding acceptable types of identity evidence can be found in the policy.

SA-22* System and services acquisition: Replace system components when the support is no longer available from developer, vendor, or manufacturer; or obtain alternative sources of support for unsupported components (e.g. original manufacturer support or original contracted vendor support). Exceptions to replacing system components include systems that provide critical mission or business capabilities where newer technologies are not available or where systems are so isolated that installing replacement components is not an option.

SI-1* System and Information Integrity Policy and Procedures: This requirement of the policy requires each agency to have a system and information integrity policy and procedures. This policy must be disseminated to all personnel with system and information integrity responsibilities and system owners. These policies and procedures must be reviewed/ updated annually and after a security incident occurs. Sample policies are available on WILENET.

SI-2 Flaw remediation: New requirements included in this section of policy include defining timetables for security relevant software and firmware updates to be made. "Critical" priority flaws must be remediated within 15 days, "High" priority flaws must be remediated within 30 days, "Medium" priority flaws must be remediated within 60 days, and "Low" priority flaws must be remediated within 90 days. Flaw remediation must be integrated into organizational configuration management process, including quarterly vulnerability scans to determine if system components have applicable security relevant updates. Agencies are also required to test software and firmware updated related to flaw remediation for effectiveness and potential side effects prior to installation.

SI-3 Malicious code protection: Malicious code protection has been expanded to include implementation of signature based malicious code protection at system entry and exit points. Blocking or quarantining malicious code, taking mitigation actions and when necessary, following the agency incident response procedures; including sending notifications to system/network administrators and/or organizational personnel with information security responsibilities. The receipt of false positives during malicious code detection and removal must be addressed to determine the impact on the availability of the system.

SI-4 System monitoring: SI-4 contains requirements to monitor the system for attacks and indicators or potentiation attacks, unauthorized network access and unauthorized use of the system using the following tools: intrusion detection and prevention, malicious code protection, vulnerability scanning, audit record monitoring, network monitoring, firewall monitoring and event logging. Agencies must provide logs to organizational personnel with information security responsibilities weekly to analyze

*Sanctionable for audit beginning October 1, 2027

detected events and anomalies. System monitoring levels should be adjusted when there is a change of risk to the organizational operations and assets, individuals, other organizations, or the nation. Agencies are required to obtain legal opinion regarding system monitoring.

SI-5 Security alerts, advisories, and directives: A new requirement has been added to this section of policy which requires agencies to implement security directives issued from external sources, (e.g., Cybersecurity and Infrastructure Security Agency (CISA), Office of management and budget, state agencies etc.) in accordance with established timeframes or to notify the issuing organization of the degree of non-compliance.

SI-7 Software, firmware, and information integrity: SI-7 introduces new compliance measures which require agencies to employ integrity verification tools which detect unauthorized changes to software, firmware, and information systems. Integrity checks can be completed at transitional states defined by the agency, (e.g., shutdown or restart of system) or other security relevant events using automated systems, or if conducted manually on weekly basis. If unauthorized changes are detected, notify your agency's system administrator. Incorporate detection of unauthorized changes to established configuration settings and unauthorized elevation of system privileges into the agency's incident response procedures.

SI-8* Spam protection: Additional requirements have been added which require daily automatic updates to spam protection mechanisms.

SI-10 Information input validation: This new compliance item requires that agencies check the validity of information inputs to web applications, servers, database servers and any system that may receive or process CJI.

SI-11* Error handling: SI-11 introduces two new requirements. Error messages created by the agency must not contain information that could be used to exploit the system and error messages can only be revealed to personnel with information security responsibilities.

SI-12 Information management and retention: A new compliance area was added to SI-12. SI-12(2) *Agencies shall use techniques to minimize the use of PII such as data obfuscation, randomization, anonymization or use synthetic data for research, testing or training.

SI-16* Memory Protection: Address space lay randomization and data execution prevention are two new requirements created in SI-16

MA-1* Maintenance policy and procedures: MA-1 requires each agency to have a system maintenance policy and procedures. This policy must be disseminated to all personnel with system maintenance responsibilities. These policies and procedures must be reviewed/ updated annually and after a security incident occurs**.** Sample policies are available on WILENET.

*Sanctionable for audit beginning October 1, 2027

MA-2* Controlled maintenance: This new policy area requires that agencies schedule, document and review records of maintenance, repair, or replacement of system components in accordance to manufacture or vendors specification or agency requirements. Maintenance records must contain the following: component name, component serial number, date/time of maintenance, maintenance performed and names of entity performing maintenance and name of escort if applicable.

Personnel with maintenance responsibilities must approve and monitor all maintenance activities whether the system or system components are serviced on site or removed to another location and approve of removal of system components for offsite maintenance, repair or replacement. Equipment must be sanitized to remove information from associated media prior to removal. After maintenance is completed, personnel with maintenance responsibility must verify potentially impacted controls are still functioning.

MA-3* Maintenance tools: The new compliance areas of MA-3 require agencies approve, control, and monitor the use of system maintenance tools and review previously approved system maintenance tools prior to each use. Agencies must prevent the removal of maintenance equipment which contains organizational information from the facility.

MA-4* Non-local maintenance: This new compliance area contains multiple requirements. Non-local maintenance and diagnostics must be approved and monitored by organizational personnel with system maintenance responsibilities. Tools used for non-local maintenance must be consistent with organizational policy and documented in the system security plan. When establishing a non-local maintenance session strong authentication (replay resistant authenticators and multi-factor authentication) must be used, maintenance records must be kept for non-local maintenance and the session terminated after maintenance is completed**.**

MA-5* Maintenance Personnel: MA-5 requires that agencies establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations and designate organizational personnel with required access authorization and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

MA-6* Timely Maintenance: Obtain maintenance support and/or spare parts for critical system components that process store or transmit CJI with an agency defined recovery period.

5.9.4 Updates

AU-1* Auditing and accountability policy and procedures: Develop and implement agency policies and procedures for auditing and accountability. The policy is to be

*Sanctionable for audit beginning October 1, 2027

disseminated to agency personnel with audit and accountability responsibilities. Review and update the policy annually and following any security incidents involving unauthorized access to CJI or systems which transmit, process or store CJI. Sample policies are available on WILENET.

AU-3(3) * Content of audit records: Limit personally identifiable information in audit records to the minimum necessary to achieve the purpose for which it was collected.

AU-4* Audit log storage capacity: Allocate adequate storage capacity to allow for a minimum of one year of audit logs to be stored.

AU-6(1) & (3) * Audit record review, analysis and reporting: Utilize automated tools for audit record review, analysis and reporting. Correlate and analyze audit records for an organization wide situational awareness.

AU-7 Audit records reduction and report generation: Utilize tools which summarize audit logs to create reports. Reporting tools must not alter the content or time data of the original log.

AU-9(4) * Protection of audit information: Limit access to management of audit logging functions to personnel with audit and accountability responsibilities, and network administrators.

AU-11 Audit record retention: Retain audit records for a minimum of one year or until it is no longer needed for administrative, legal, audit, or other operational purposes to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

AU-12 Audit Record Generation: Provide the capability for detailed audit records to be created from logged events. Personnel with information security responsibilities should select the event types to be logged by specific components to the system.

PE-1* Physical and Environmental Protection and procedures: Develop and implement agency policies and procedures for physical and environmental protection. Review and update the policy annually and following any security incidents involving unauthorized access to CJI or systems which transmit, process or store CJI. Sample policies are available on WILENET.

PE- 8* Visitor access records: Maintain visitor access records for one year. Review the records quarterly and report anomalies to personnel with information security responsibilities. Visitor records should limit personally identifiable information collected to the minimum required.

PE-9* Power cabling and equipment: Protect power equipment and power cabling for the system from damage and destruction.

*Sanctionable for audit beginning October 1, 2027

PE-10* Emergency Shutoff: Provide the capability to shut off all information systems in the event of an emergency. Ensure the shut switches or devices are protected from unauthorized access but remain easily accessible to authorized personnel.

PE-11* Emergency Power: Provide an uninterruptible power supply to facilitate an orderly shutdown of the information system or transition of the information system to an alternate power source in the event of a primary power source loss.

PE-12* Emergency Lighting: Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

PE-13* Fire Protection: Employ and maintain a fire detection and suppression system.

SC-1* Policy and Procedure: Develop and implement agency policies and procedures for system and communication protection. Review and update the policy annually and following any security incidents involving unauthorized access to CJI or systems which transmit, process or store CJI. Sample policies are available on WILENET.

SC-4 Information in shared system resources: Prevent unauthorized and unintended information transfer via shared system resources.

SC-5* Denial of service protection: Protect against denial-of-service attacks e.g. distributed denial of service attack by utilizing a boundary protection device (firewall) and an intrusion detection or prevention system.

SC-7 Boundary protection: Limit the number of external network connections to the system and implement a managed interface for each telecommunication service. Each managed interface should have a traffic flow policy, protecting the confidentiality and integrity of data being transmitted through the interface. Document any exception to the traffic flow policy with a supporting business need. Review exceptions annually and after security incidents and remove exceptions when no longer needed. Prevent unauthorized exchange of control plane traffic with external networks. Publish information to enable remote networks to detect unauthorized control plan traffic from internal networks and filer unauthorized control plane traffic from external networks.

SC-10* Network Disconnect: Terminate network connections at the end of the session or after one hour of inactivity. This requirement does not apply to dispatch workstations (within the physically secure location) or part of a criminal justice conveyance.

SC-15* Collaborative computing devices: Collaborative computing devices (e.g. smartboards, remote meeting devices, etc.) may not be activated remotely; the devices must provide explicit indication of use to personnel present at the device.
SC-18* Mobile Code: Authorize, monitor and control acceptable mobile code technology (e.g. interface technology) within the system.

*Sanctionable for audit beginning October 1, 2027

SC-20 Secure Name/Address Resolution Service: Provide additional data origin authentication and integrity verification artifacts along with authoritative name resolution in response to external name/ address queries. Provide the means to indicate security status of child zones.

SC-21 Recursive or caching resolvers: Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

SC-22* Architecture and provisioning for name/address resolution service: If hosting DNS services, ensure the system is fault tolerant and implement internal / external role separation.

SC-23* Session Authenticity: Protect the authenticity of communication sessions.

PL-1* Planning policies and procedures: Develop and implement agency policies and procedures for planning. Review and update the policy annually and following any security incidents involving unauthorized access to CJI or systems which transmit, process or store CJI. Sample policies are available on WILENET.

PL-2* System security and privacy plan: Develop a security and privacy plan for your agency's system. The plan should clearly describe the system and the type(s) of information which are handled. Identify risks and potential threats to the system and data processed. Determine appropriate control measures to mitigate risks and threats and document them in the plan. Disseminate the plan to appropriate agency personnel and ensure the plan is protected from unauthorized access. Review the plan annually or when required due to system changes.

PL-4* Rules of Behavior: Develop rules of behavior for system users. Obtain documentation of acknowledgement from system users before granting access to the system and annually thereafter or after changes to the rules of behavior. Review rules of behavior annually. Rules of behavior should include restrictions on use of social media for official duties, posting organizational information on public websites and using organization provided identifiers and authentication secrets (passwords) on external sites / applications.

PL-8* Security and privacy architecture: Develop system architecture to protect the confidentiality, integrity and availability of system information. Review and update the architecture at least annually or when changes to the system environment occur.

CP-1* Contingency planning policies and procedures: Develop and implement agency policies and procedures for contingency planning. Review and update the policy annually and following any security incidents involving unauthorized access to CJI or systems which transmit, process or store CJI. Sample policies are available on WILENET.

*Sanctionable for audit beginning October 1, 2027

CP-2* Contingency plan: Develop a contingency plan for your agency. Define contingency plan objectives, determine essential mission function and integrate incident handling into the contingency plan. The contingency plan should allow for essential mission function to resume within twenty-four (24) hours of the plan being activated. The contingency plan should be reviewed by agency leadership (or a designee) and disseminated to the appropriate agency personnel. Review the contingency plan annually.

CP-3* Contingency training: Provide contingency plan training to system users consistent with their assigned roles and responsibilities. Complete training within thirty (30) days of assignment to role with contingency plan responsibilities, or when required by system changes and annually thereafter. Contingency training content should be updated annually or after a security incident results in unauthorized access to CJI or contingency planning training.

CP-4* Contingency plan testing: Test your contingency plan for effectiveness by using checklists, walk-though, tabletop exercises and simulation. Review the results of the contingency plan and initiate any corrective actions if necessary.

CP-6* Alternate storage site: Establish an alternate storage site separated sufficiently from the primary site to reduce susceptibility to the same threats. The alternate storage site should have the same protection as the primary storage site. The alternate storage site should be sufficiently separated from the primary storage site and assessed for accessibility issues from a region wide disruption.

CP-7* Alternate processing site: Identify an alternate processing site separated sufficiently from the primary site to reduce susceptibility to the same threats and assessed for accessibility issues from a region wide disruption. The alternate processing site should be equipped with required equipment and supplies to transfer and resume operation within the timeline established in the contingency plan.

CP-8* Telecommunication services: Establish alternate telecommunication services, develop telecommunication service agreements that contain priority-of-service provisions and request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

CP-9* System Backup: Test system backup as required by agency contingency plan. System backups must be encrypted to prevent unauthorized access.

CP-10* System recovery and reconstitution: Recover your agency's system to a known state within the timeline defined in the contingency plan after a disruption, compromise or failure.

RA-1* Risk assessment policies and procedures: Develop and implement agency policies and procedures for risk assessment. Review and update the policy annually

*Sanctionable for audit beginning October 1, 2027

and following any security incidents involving unauthorized access to CJI or systems which transmit, process or store CJI. Sample policies are available on WILENET.

RA-2* Security Categorization: Categorize the system and the information it processes, stores, and transmits. The CJIS security policy has assigned a "moderate" categorization for criminal justice information. If your agency uses other security categorizations for non CJI data, provide the rationale for that data's categorization in the agency security plan.

RA-3* Risk Assessment: Conduct a risk assessment of your agency's system. Identify possible vulnerabilities and threats to the systems and determine the likelihood and magnitude of harm from unauthorized access to, disruption, modification, or deletion of the system. Review the results of the risk assessment quarterly and disseminate to personnel with risk assessment and security/privacy responsibilities.

RA-5 Vulnerability monitoring and scanning: Monitor and scan for vulnerabilities in the system and hosted applications at least monthly and when new vulnerabilities potentially affecting the system are identified and reported. Vulnerability scanning tools should utilize standards for enumerating platforms, software flaws and improper configurations. Remediate legitimate vulnerabilities within the timelines listed with the CJIS security policy. Update system vulnerabilities to be scanned within twenty-four hours of the scan running to ensure all new vulnerabilities are identified and reported.

RA-7* Risk Response: Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

RA-9* Criticality Analysis: Identify critical system components and functions by performing a criticality analysis for information system components containing or processing CJI at the planning, design, development, testing, implementation, and maintenance stages of the system development life cycle.

5.9.5 Updates

CM-1* Configuration management policy and procedures: Develop and implement agency policies and procedures for configuration management. Review and update the policy annually and following any security incidents involving unauthorized access to CJI or systems which transmit, process or store CJI. Sample policies are available on WILENET.

CM-2 Baseline configuration: Utilize tools such as configuration management tools, firmware inventory management tools, etc. to maintain ensure baseline configuration documentation is current, accurate and available. At least one version of the baseline configuration shall be maintained to support a system rollback.

CM-3* Configuration control change: Determine and document system changes which are configuration controlled, review proposed changed and document the results

*Sanctionable for audit beginning October 1, 2027

of configuration change decisions. Implement changes and maintain records of the changes for a minimum of two years. Monitor and review the results of the changes and coordinate with personnel with configuration management responsibilities. Changes to the system should be tested and validated before finalizing the implementation. Include organization personnel with information security and privacy responsibilities in configuration change decisions.

CM-4* Impact Analyses: Analyze changes to the system and determine potential security and privacy impacts prior to implementing system changes. After the changes have been implemented, verify that they are functioning as intended.

CM-5 Access Restriction for change: Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

CM-6 Configuration Settings: Establish, document and implement configuration settings for system components. These settings should be the most restrictive while still meeting your agency's operating requirements. Utilize established best practice guidelines such as Defense Information Systems Agency (DISA), Secure Technical Implementation Guidelines (STIGs), Center for Internet Security (CIS) Benchmarks, or Federal Information Processing Standards (FIPS). If any exceptions are made to the established configuration settings, document and approve these deviations. Monitor and approve change to the configuration settings in accordance with your agencies policies and procedures.

CM-7 Least functionality: Configure system to provide only essential capabilities to meet your agency's operational needs. Prohibit or restrict the use of specified functions, ports, protocols, software, and/or services which are not required. Review configuration annually, after system changes or after a security incident to identify unnecessary or unsecure elements of the configuration and disable those elements.

CM-8 System Component Inventory: Develop and document an inventory of system components. Inventory should include date of installation, model, serial number, manufacturer, supplier information, component type, software owner, software version number, software license information, and hardware and physical location. System component inventory should be reviewed and updated annually. When new components are added to the system or components are removed, make sure the system component inventory is updated. Utilize tools to detect the presence of unauthorized hardware, software and firmware in an automated manner continuously or at least weekly. If unauthorized components are detected, notify appropriate organizational personnel and disable or isolate the component.

CM-9* Configuration management plan: Develop and implement a configuration management plan for your agency. Protect the plan from unauthorized disclosure and modification. Review the plan and ensure it is approved by agency personnel with information security and configuration management responsibilities.

*Sanctionable for audit beginning October 1, 2027

CM-10* Software usage restrictions: Use software and associated documentation in accordance with contract agreements and copyright laws. Keep track of software license usage to ensure software is not being illegally shared. Manage and document the use of peer-to-peer sharing platforms to ensure it is not used for unauthorized purposes.

CM-11* User installed software: Create agency policy regarding user installed software. Utilize automated processes to enforce the policy and monitor policy compliance on a weekly basis**.**

CM-12* Information location: Identify and document the location of CJI, and specific system component which processes, transmits or stores that information. Document location changes of those systems or system components. Utilize automated tools to identify CJI on software and hardware system components to ensure proper controls are in place to protect the data.

6.0 Updates

CA-7 Continuous Monitoring: Assess effectiveness of the controls listed in the CJIS security policy at agency defined intervals which are sufficient to make an adequate assessment for risk-based decision making. Employ independent assessors or assessment teams to monitor controls in the system on a continuous basis.

Reminders

Fixing priority 1 items that are currently out of compliance will greatly reduce an agency's vulnerability to a cyber security incident. Review either the CJIS Security Policy or the Requirement Companion Document for a list of controls, their priority and sanction date to determine where to focus your agency's attention and resources.

If your agency has a Records Management System (RMS) and/or CAD/NCIC interface software application, your agency is required to incorporate the CJIS Security Policy into contracts with the vendor. It is also recommended that language is included in the contract that the vendor will abide by the most up-to-date version of the CJIS Security Policy.

Any prospective changes to your agency's network/systems should be contemplated and planned with the CJIS Security Policy as your guide to ensure you are making changes that are compliant with the policy.

The most current version of the CJIS Security Policy and its accompanying Companion Document can be found at: CJIS Security Policy Resource Center — LE

*Sanctionable for audit beginning October 1, 2027

Local Agency Security Officer Training Certification Statement

I certify that I have read and understand the contents of the Local Agency Security handout and agree to follow all TIME/CJIS Systems requirements regarding the roles and responsibilities including, but not limited to the following:

- Identify who is using the Crime Information Bureau approved hardware, software and firmware and ensure no unauthorized individuals or processes have access to the system.
- Identify and document how the equipment is connected to the state system.
- Ensure that all personnel security screening procedures are being followed as stated in the CJIS Security Policy.
- Ensure the approved and appropriate security measures are in place and working as expected.
- Support policy compliance and ensure the Wisconsin Information Security Officer is promptly informed of security incidents.

I also understand that the criminal justice information made available via the TIME/CJIS Systems is sensitive and has potential for great harm if misused; therefore, access to this information is limited to authorized personnel. I understand that misuse of the TIME/CJIS systems or information received from these systems may subject me to system sanctions/penalties and may also be a violation of state or federal laws, subjecting me to criminal and/or other penalties. Misuse of the TIME/CJIS Systems includes accessing the systems without authorization or exceeding my authorized access level, accessing the systems for an improper purpose, using, or disseminating information received from the systems for a non-work related or non-criminal justice purpose, etc.

Your signature: _____

Print your name: _____

Agency Name: _____

Date: _____