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). Examples of CJI that should be protected include:

- 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 individual,
- 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 but not later than six months after initial assignment, 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.

[1] sanctionable for audit beginning October 1, 2024.

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 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., virtually) 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 and appear on the agency's authorized user list.

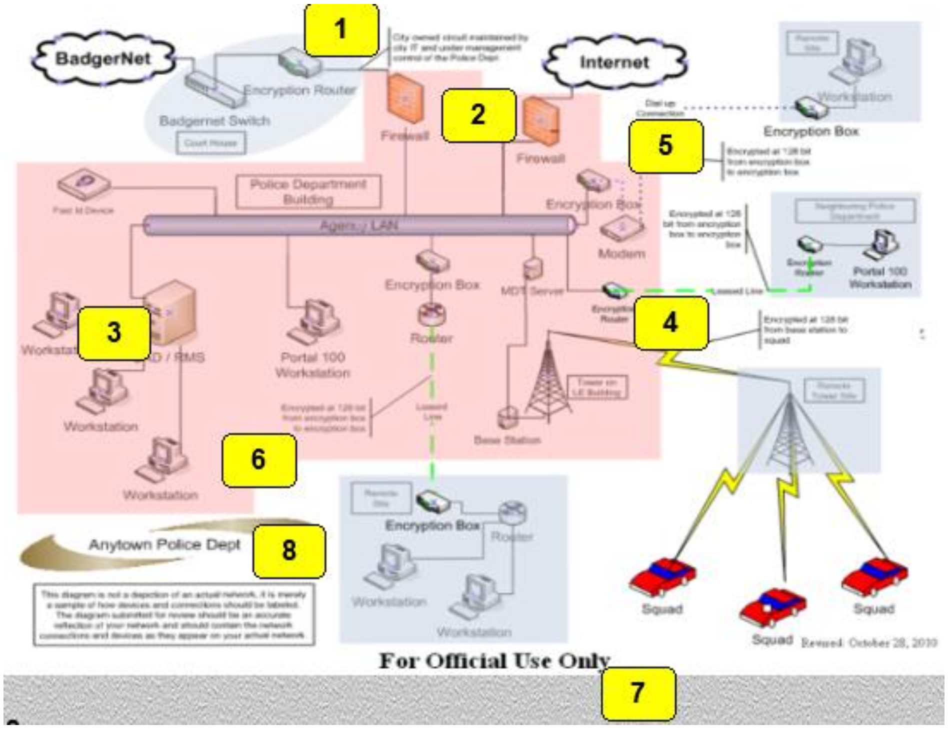
Agencies should keep all hardware and software up-to-date and ensure any encryption meets the CJIS Security Policy requirements.

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.

[1] sanctionable for audit beginning October 1, 2024.

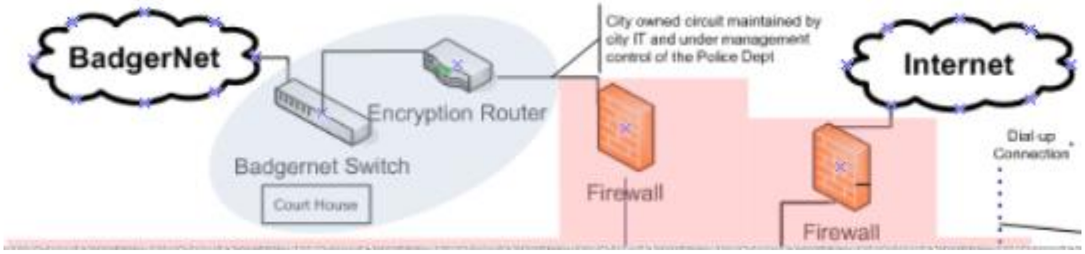


This diagram is not a depiction of an actual network, it is merely a sample of how devices and connections should be labeled. The diagram submitted for review should be an accurate reflection of your network and should contain the network connections and devices as they appear on your actual network.

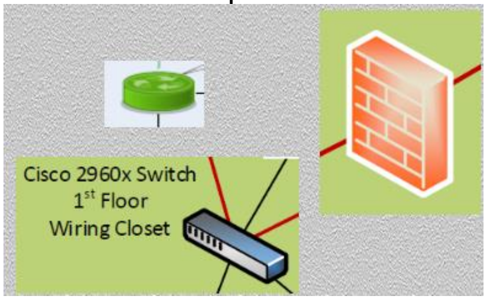
Revised: October 28, 2010

For Official Use Only

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.



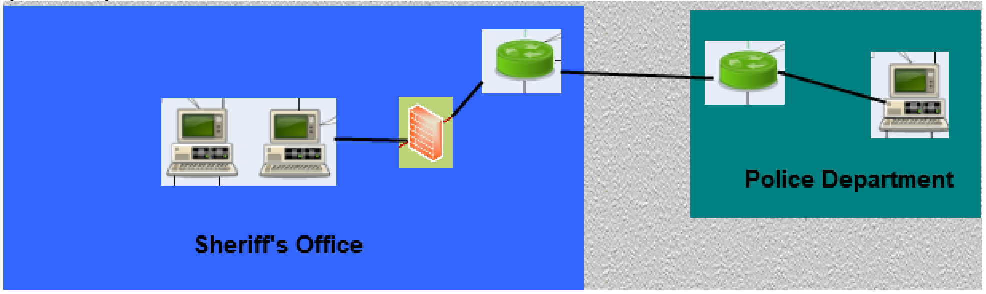
2. Depict all entry points into the network including any hardware components that are used to isolate the network from other networks at the agency (hardware that should be depicted includes firewalls, switches, routers, servers, etc.).



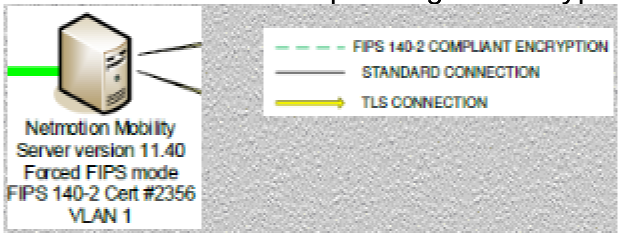
3. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations

[1] sanctionable for audit beginning October 1, 2024.

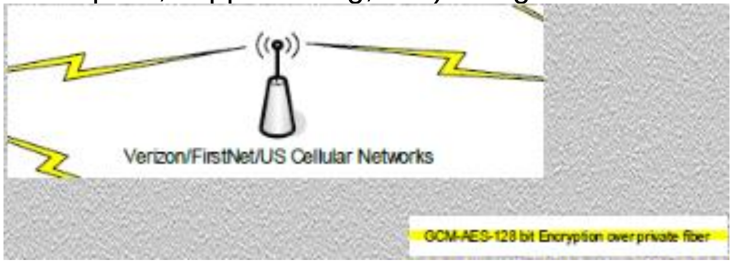
(clients) do not have to be shown; the number of clients is sufficient.



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.



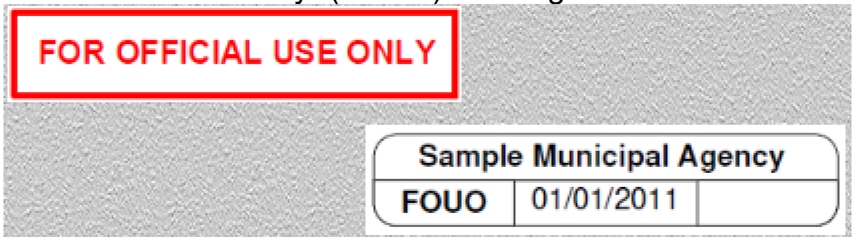
5. Identify the transmission methods (data circuit, microwave, cellular technologies, fiber optics, copper wiring, etc.) being used to transmit or receive TIME/CJIS data.


Verizon/FirstNet/US Cellular Networks
GCM-AES-128 bit Encryption over private fiber

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

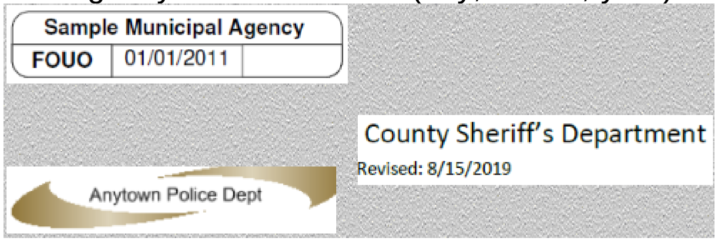
Sheriff's Office

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



[1] sanctionable for audit beginning October 1, 2024.

8. The agency name and date (day, month, year) 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 should 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 should be conducted for warrants and if the person is not a Wisconsin resident, a search of the out-of-state's criminal history repository should 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 area 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.

[1] sanctionable for audit beginning October 1, 2024.

- 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 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.

As the 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 CIBTSCC@doj.state.wi.us or calling 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 below findings 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 in compliance with 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,

[1] sanctionable for audit beginning October 1, 2024.

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 and agencies 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.

Agencies that access CJI outside of the physically secure location(s) or controlled area(s) must have Advanced Authentication, also called Multifactor Authentication (MFA) deployed. Any device that accesses CJI from outside the physically secure location or controlled area must have MFA deployed. This can be on laptops, smartphones, tablets, or desktops, etc. The LASO should determine what the physically secure location(s) and/or controlled area(s) of the agency are. Then, the agency can determine whether any devices fall outside of those boundaries to deploy MFA on those devices. Updates to the CJIS security policy require that all devices which can access, transmit or process CJI must have multi factor authentication.

Another area where agencies are not compliant with the requirements of the CJIS Security Policy are intrusion detection systems (IDS) 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, it must be encrypted with a FIPS 140-2 certified encryption algorithm if the CJI leaves the physically secure location. Many agencies' responses to the audit indicate that they do not encrypt electronic transmission of CJI, or the encryption is "FIPS compliant", both of which do not meet the FIPS 140-2 certified standard that is required. If your agency currently has encryption, you should reach out to the vendor and

[1] sanctionable for audit beginning October 1, 2024.

ask for the FIPS 140-2 certificate that covers the encryption. If one cannot be produced, the agency must find a FIPS 140-2 certified method of encryption to deploy. If your agency has not yet implemented encryption, be sure to get the FIPS 140-2 certificate that covers the encryption you plan to implement prior to purchasing it to ensure it is compliant.

Temporary remote access is access to an agency's network or systems that is outside of the agency's physically secure location. This can be done by the agency, IT, or vendor/contractor personnel on a temporary basis for maintenance or troubleshooting. Any temporary remote access must meet certain requirements to ensure it complies with the CJIS Security Policy. All temporary remote access must be done in a manner that is FIPS 140-2 certified encrypted. "FIPS compliant" is not enough to satisfy this requirement. Temporary remote personnel must be either virtually escorted or have Multifactor Authentication implemented. Virtual escorting is a means by which an agency verifies the temporary remote personnel. It includes meeting these criteria:

1. The session must 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 (or MFA) solution or during the session via active teleconference with the escort throughout the session.

All requirements of virtual escorting must be met to be considered virtual escorting. If this cannot be done, then Multifactor Authentication must be used during the session. It is possible for an agency to not use temporary remote access at all on their network. This would require that all maintenance and troubleshooting be done on-site at the agency.

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 within six months of appointment and annual thereafter. Currently, LASO training is available via online module only.

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 140-2 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

[1] sanctionable for audit beginning October 1, 2024.

the entry is still valid (warrant is still outstanding, missing person still missing, property still missing/stolen, etc.).

Wisconsin was audited by the FBI in 2022. There were several findings on the audit, broken into the Information Technology (ITS) and NCIC categories. Findings on the ITS audit include:

- Criminal justice agencies that have non-criminal justice entities performing IT or contracted services (including dispatch functions) do not have signed CJIS Security Addendums on file for all personnel.
- Agencies do not have written policies for physical protection requirements and have not implemented the requirements for physical protection.
- 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 do not have a written policy for account management and identification procedures. Agencies do not have a policy to document the validation process of system accounts.
- 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 Advanced Authentication (also known as Multifactor Authentication) is implemented for personnel who access or manage information systems accessing CJI from non-secure locations.
- Agencies are not ensuring CJI transmitted or stored outside the boundary of the physically secure location is protected via encryption.
- Agencies are not ensuring additional protections are implemented for metadata derived from CJI accessed or stored within a third-party cloud environment.
- Agencies do not have a security incident response policy documented and implemented.

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

- Agencies are not placing Locates on corresponding NCIC records after hit confirmation.
- Agencies are not removing protection orders appropriately (clear vs. cancel).
- Agencies are not ensuring the use and dissemination of Interstate Identification Index (III) information is authorized.

Changes to the CJIS Security Policy

The FBI has started a multi-year revamp of the CJIS Security Policy. Each section of the policy will be updated until the whole policy has been rewritten. There will also be new policy sections. Version 5.9.3 was released on September 14, 2023.

[1] sanctionable for audit beginning October 1, 2024.

Version 5.9.1 updated the language in Section 5.12 Personnel Security and Appendix G.3: Cloud Computing. The language change affects criminal justice agencies that use a cloud provider. The new language in Appendix G.3 Cloud Computing makes a distinction between types of cloud services Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Agencies must understand the type of service they have and if their service allows the cloud company to access CJI. The language update in the personnel security section states that fingerprint-based record checks may not be required for all cloud provider personnel depending on the type of service offering (IaaS, PaaS, or SaaS) and access to encryption keys. If an agency uses a service model where cloud provider personnel have no access to unencrypted CJI or to encryption keys, then the fingerprint-based background check is not required. Any unescorted access to unencrypted CJI still requires a fingerprint-based background check.

The biggest change to Version 5.9.1 was the update to Section 5.8 Media Protection. This section was the first to be rewritten in the new format and all future updates will carry this new format. The policy breaks Media Protection into different categories with the controls (requirements) and a discussion. The changes that were made to Section 5.8 became sanctionable on October 1, 2023.

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 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

[1] sanctionable for audit beginning October 1, 2024.

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 the 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[1]: Updates to section 5.3 Incident response policy and procedures requires that the agency's incident response policy and procedures are reviewed/updated annually and after a security incident occurs.

IR-2(3)b* Incident response training[1]: Provide incident response training to agency personnel consistent with a user's assigned roles and responsibilities. Review and update the incident response training content annually.

IR-3 Incident response testing[1]: 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.

[1] sanctionable for audit beginning October 1, 2024.

IR-8(1) Incident response plan / breaches[1]: 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[1]: 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[1]: Updates to this section of policy requires 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/ 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[1]: Updates to section AC-7 defines 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[1]: 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[1]: Agencies shall determine actions that can be performed without identification or authentication. Document and provide rationale for in the security plan for actions which do not require identification/authentication.

AC-20 Use of external systems[1]: Updates to section AC-20 prohibit the use of personally owned information systems (including mobile devices) and publicly accessible system for accessing, processing, storing, or transmitting CJI.

AC-22 Publicly accessible content[1]: 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[1]: This update to the policy require each agency to have an identification and authentication policy and procedures. This policy must be disseminated to all personnel with unescorted access to

[1] sanctionable for audit beginning October 1, 2024.

CJI. These policies and procedures must be reviewed/ updated annually and after a security incident occurs.

IA-2 Identification and authentication of organizational users[1]: 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[1]: Uniquely identify and authentication 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[1]: 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[1]: 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[1]: Implement mechanisms for authentication before granting access to cryptographic module that meet executive orders, directive, policies, regulations, standards, and guidelines for such authentication.

IA-8 Identification and authentication (non-organization users) [1]: Uniquely identify and authenticate non-organization users or processes acting on their behalf. Ensure that only NIST compliant external authenticators are accepted by your agency, 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[1]: Require users to re-authenticate when roles, authenticators, or credentials change, when privileged functions are executed or every 12 hours.

IA-12 Identity proofing[1]: 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.

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 un-supported components (e.g. original manufacturer support or original contracted vendor support). Exceptions to replacing system components includes 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.

[1] sanctionable for audit beginning October 1, 2024.

SI-1 System and Information Integrity Policy and Procedures: This new requirement of the policy require 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.

SI-2 Flaw remediation: New requirements included in this section of policy includes 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 detected events and anomalies. System monitoring levels should be adjusted of 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

[1] sanctionable for audit beginning October 1, 2024.

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. 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[1]: 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**.**

MA-2 Controlled maintenance[1]: 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[1]: 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

[1] sanctionable for audit beginning October 1, 2024.

removal of maintenance equipment which contains organizational information from the facility.

MA-4 Non-local maintenance[1]: 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[1]: 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 require access authorization and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

MA-6 Timely Maintenance[1]: Obtain maintenance support and/or spare parts for critical system components that process store or transmit CJI with an agency defined recovery period.

Reminder:

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 can be found at: CJIS Security Policy v5.9.3 2023-09-14 — LE (fbi.gov).

[1] sanctionable for audit beginning October 1, 2024.

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: ____