State of Wisconsin –

IT Security Standards Handbook

Effective Date: August 1, 2025

TABLE OF CONTENTS

OVERVIEW

Pursuant to the Wisconsin Department of Administration's ("DOA") Statutory authority in Chapter 16 of the Wisconsin Statutes, DOA's Division of Enterprise Technology ("DET"), in collaboration with executive branch agencies, has developed the State of Wisconsin IT Security Standards Handbook to establish security standards for the administration of information technology services.

As provider of the State's consolidated, executive branch data center services, which require compliance with a multitude of federal and State regulatory requirements, DOA has adopted the NIST Risk Management Framework ("RMF") as the foundational framework for the creation of executive branch IT security policies and standards. The RMF integrates security, privacy, and cyber supply chain risk management activities into a comprehensive system development life cycle. The RMF links to a suite of NIST standards and guidelines to support implementation of risk management programs to meet the requirements of the Federal Information Security Modernization Act (FISMA). This risk-based approach to control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, and regulations.

The State of Wisconsin IT Security Standards Handbook has been developed from the National Institute of Standards and Technology ("NIST") Special Publication 800-53, Revision 5 (NIST SP 800-53, rev 5). This addresses diverse security and privacy requirements and establishes recommended baseline security controls for government organizations. DOA has adopted all designated low and moderate level controls (Baseline) from NIST Special Publication 800-53, Revision 5 as a minimum requirement for executive branch agencies. Selected high level controls (Regulatory) may also be applicable depending on federal regulations. Agencies shall categorize their data, identify the potential impact (high, moderate, or low), and select the appropriate controls by using Table 3-1 in NIST Special Publication 800-53B. Agencies are required to update DET on the status of their control implementation through the bi-annual reporting and monitoring process.

Executive branch agencies are responsible for identifying and implementing all appropriate policies, procedures, or processes for their state information systems and system environments to protect State information. **Note:** Some agencies have more stringent regulatory requirements which exceed the control baseline required for all executive branch agencies. Implementation of the controls can be (1) a common (inheritable) control, (2) a system-specific control, or (3) a hybrid control. The control implementation defines the scope of applicability for the control, the shared nature or inheritability of the control, and the responsibility for control development, implementation, assessment, and authorization.

METHODOLOGY FOR CONTROL SELECTION

DOA used the following methodology to select the baseline and regulatory controls included in the standards.

- A matrix was created that lists the NIST Special Publication 800-53, Revision 5 controls.
- The following regulatory requirements were also included in the matrix:
  - IRS Publication 1075 (rev 11/21)
  - MARS-E v. 2.2
  - CJIS v. 6.0
  - HIPAA Security Rule 45 C.F.R.
  - FERPA
  - ISO 270001
  - PCI-DSS v4.0.1
- Table 3-1 of NIST SP 800-53B was used to identify the impact levels (high, moderate, low) for controls and control enhancements.

- For baseline controls, all designated low and moderate level controls from NIST SP 800-53, rev 5 were selected.
- Using the matrix, certain high-level controls and controls without a NIST rating were selected as regulatory controls. Controls selected for regulatory controls applied to multiple compliance requirements.

100 Access Control Standard

Purpose

The Access Control Standard provides documentation of the minimum Access Control requirements for access to Executive Branch Agencies Information Technology (IT) systems and system environments. This standard is intended to facilitate the attainment of the Access Control Policy, the Configuration Management Policy and Standard, the Identification and Authentication Policy and Standard, the Personnel Screening Policy and Standard, and associated Information Technology (IT) Security Policy objectives (AC-01, CM-01).

This standard is divided into two sections of controls. **Section One** contains the minimum baseline controls that Executive Branch agencies shall implement. **Section Two** contains some of the common, regulatory controls agencies may be required to implement in addition to the baseline controls. Section Two is not all-inclusive. Each agency is responsible for identifying what other controls their agency may be required to implement beyond the scope of this standard.

SECTION ONE: BASELINE CONTROLS

Policy and Procedures (AC-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
  - An access control policy that:
    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
  - Procedures to facilitate the implementation of the access control policy and the associated access controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the access control policy and procedures.
- Review and update the current access control:
  - Policy on an agency-defined frequency.
  - Procedures on an agency-defined frequency.

Account Management (AC-2):

- Define and document the types of accounts allowed and specifically prohibited for use within the system. (Examples of account types include individual, shared, group, system, guest, emergency, developer, temporary, and service).
- Assign account managers.
- Require conditions for group and role membership.
- Specify:
  - Authorized users of the system.
  - Group and role membership.
  - Access authorizations (i.e., privileges) and other attributes (as required) for each account.
- Require approvals by agency-defined personnel or roles for requests to create accounts.
- Create, enable, modify, disable, and remove accounts in accordance with agency-defined policies, procedures, prerequisites, and criteria.

- Monitor the use of accounts.
- Notify account managers and appropriate agency personnel or roles:
    - Immediately when accounts are no longer required.
    - Immediately when users are terminated or transferred.
    - Immediately when system usage or need-to-know changes for an individual.
- Authorize access to the system based on:
    - A valid access authorization.
    - Intended system usage.
    - Agency-defined attributes (as required).
- Review accounts for compliance with account management requirements on an agency-defined frequency.
- Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group.
- Align account management processes with personnel termination and transfer processes.

Account Management | Automated System Account Management (AC-2(1)):

- Support the management of system accounts using automated mechanisms.

Account Management | Automated Temporary and Emergency Account Management (AC-2(2)):

- Automatically remove/disable temporary and emergency accounts after an agency-defined time period for each type of account.

Account Management | Disable Accounts (AC-2(3)):

- Disable accounts within 120 days when the accounts:
    - Have expired.
    - Are no longer associated with a user or individual.
    - Are in violation of agency policy.
    - Have been inactive for 120 days.

Account Management | Automated Audit Actions (AC-2(4)):

- Automatically audit account creation, modification, enabling, disabling, and removal actions.

Account Management | Inactivity Logout (AC-2(5)):

- Require that users log out when there is an agency-defined time period of expected inactivity or before leaving the system unattended.

Account Management | Disable Accounts for High-Risk Users (AC-2(13)):

- Disable accounts of individuals immediately upon discovery of significant security or privacy risks.

Access Enforcement (AC-3):

- Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Access Enforcement | Individual Access (AC-3(14)):

- Provide mechanisms to enable individuals to have access to agency-defined elements of their personally identifiable information.

Information Flow Enforcement (AC-4):

- Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on information flow control policies.

Separation of Duties (AC-5):

- Identify and document duties of individuals requiring separation.
- Define system access authorizations to support separation of duties.

Least Privilege (AC-6):

- Employ the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned agency tasks.

Least Privilege | Authorize Access to Security Functions (AC-6(1)):

- Authorize access for individuals or roles to:
  - Security functions deployed in hardware, software, and firmware.
  - Agency-defined security-relevant information.

Least Privilege | Non-Privileged Access for Non-Security Functions (AC-6(2)):

- Require that users of system accounts (or roles) with access to agency-defined security functions or security-relevant information use non-privileged accounts or roles, when accessing non-security functions.

Least Privilege | Privileged Accounts (AC-6(5)):

- Restrict privileged accounts on the system to agency-defined personnel or roles.

Least Privilege | Review of User Privileges (AC-6(7)):

- Review on an agency-defined frequency the privileges assigned to roles or classes of users to validate the need for such privileges.
- Reassign or remove privileges, if necessary, to correctly reflect agency mission and business needs.

Least Privilege | Log Use of Privileged Functions (AC-6(9)):

- Log the execution of privileged functions.

Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions (AC-6(10)):

- Prevent non-privileged users from executing privileged functions.

Unsuccessful Logon Attempts (AC-7):

- Enforce a limit of three (3) consecutive invalid logon attempts by a user within a 120-minute period.
- Automatically lock the account when the maximum number of unsuccessful attempts is exceeded.

System Use Notification (AC-8):

- Display an agency-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
  - Users are accessing a State of Wisconsin information system.
  - System usage may be monitored, recorded, and subject to audit.
  - Unauthorized use of the system is prohibited and subject to criminal and civil penalties.
  - Use of the system indicates consent to monitoring and recording.
- Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.
- For publicly accessible systems:
  - Display system use information before granting further access to the publicly accessible system.
  - Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.
  - Include a description of the authorized uses of the system.

Device Lock (AC-11):

- Prevent further access to the system by initiating a device lock after 15 minutes of inactivity; requiring the user to initiate a device lock before leaving the system unattended.
- Retain the device lock until the user re-establishes access using established identification and authentication procedures.

Device Lock | Pattern-Hiding Displays (AC-11(1)):

- Cancel, via the device lock, information previously visible on the display with a publicly viewable image.

Session Termination (AC-12):

- Automatically terminate a user session after agency-defined conditions or trigger events requiring session disconnect. Conditions or trigger events that require automatic termination of the session include agency-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on system use.

Permitted Actions without Identification or Authentication (AC-14):

- Identify user actions that can be performed on the system without identification or authentication consistent with agency mission and business functions.
- Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

Remote Access (AC-17):

- See 101 Access Control for Remote Access Standard for controls related to remote access.

Wireless Access (AC-18):

- See 102 Access Control for Wireless Access Standard for controls related to wireless access.

Access Control for Mobile Devices (AC-19):

- See 103 Access Control for Mobile Device Security Standard for controls related to mobile devices.

Use of External Systems (AC-20):

- Establish terms and conditions and/or identify controls asserted to be implemented on external systems, consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:
  - Access the system from external systems.
  - Process, store, or transmit agency-controlled information using external systems.
- Prohibit the use of agency-defined types of external systems.

Use of External Systems | Limits of Authorized Use (AC-20(1)):

- Permit authorized individuals to use an external system to access the system or to process, store, or transmit agency-controlled information only after:
  - Verification of the implementation of controls on the external system as specified in the agency's security and privacy policies and security and privacy plans.
  - Retention of approved system connection or processing agreements with the agency entity hosting the external system.

Use of External Systems | Portable Storage Devices – Restricted Use (AC-20(2)):

- Restrict the use of agency-controlled portable storage devices by authorized individuals on external systems using agency-defined restrictions.

Information Sharing (AC-21):

- Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for agency-defined information sharing circumstances where user discretion is required.
- Employ automated mechanisms or manual processes to assist users in making information sharing and collaboration decisions.

Publicly Accessible Content (AC-22):

- Designate individuals authorized to make information publicly accessible.
- Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.
- Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included.
- Review the content on the publicly accessible system for nonpublic information on an agency-defined frequency and remove such content, if discovered.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies shall implement the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may also be subject to additional Federal, State, and/or Inter-agency regulatory requirements. It is each agency's responsibility to research and implement additional controls needed to meet regulatory compliance requirements and expectations outside of the State of Wisconsin baseline of controls.

Account Management | Privileged User Accounts (AC-2(7)):

- Establish and administer privileged user accounts in accordance with a role-based scheme or an attribute-based access scheme.
- Monitor privileged role or attribute assignments.
- Monitor changes to roles or attributes.
- Revoke access when privileged role or attribute assignments are no longer appropriate.

Account Management | Restrictions on Use of Shared and Group Accounts (AC-2(9)):

- Only permit the use of shared and group accounts that meet agency-defined conditions for establishing shared and group accounts.

Account Management | Account Monitoring for Atypical Usage (AC-2(12)):

- Monitor system accounts for atypical usage.
- Report atypical usage of system accounts to appropriate agency personnel or roles.

Access Enforcement | Controlled Release (AC-3(9)):

- Release information outside of the system only if:
  - The receiving system or system component provides agency-defined controls.
  - Agency-defined controls are used to validate the appropriateness of the information designated for release.

Concurrent Session Control (AC-10):

- Limit the number of concurrent sessions for each agency-defined account and/or account type to an agency-defined number.

Session Termination | User-Initiated Logouts (AC-12(1)):

- Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to agency-defined information resources.

Use of External Systems | Non-Organizationally Owned Systems – Restricted Use (AC-20(3)):

- Restrict the use of non-organizationally owned systems or system components to process, store, or transmit agency information using agency-defined restrictions.

Data Mining Protection (AC-23):

- Employ agency-defined data mining prevention and detection techniques for agency-defined data storage objects to detect and protect against unauthorized data mining.

101 Access Control for Remote Access Standard

Purpose

This standard is intended to facilitate the attainment of the Access Control Policy and associated Information Technology (IT) Security Policy objectives.

This standard is divided into two sections of controls. **Section One** contains the minimum baseline controls that Executive Branch agencies shall implement. **Section Two** contains some of the common, regulatory controls agencies may be required to implement in addition to the baseline controls. Section Two is not all-inclusive. Each agency is responsible for identifying what other controls their agency may be required to implement beyond the scope of this standard.

SECTION ONE: BASELINE CONTROLS

Remote Access (AC-17):

- Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.
- Authorize each type of remote access to the system prior to allowing such connections.

Remote Access | Monitoring and Controlling (AC-17(1)):

- Employ automated mechanisms to monitor and control remote access methods.

Remote Access | Protection of Confidentiality and Integrity Using Encryption (AC-17(2)):

- For systems and data identified as moderate risk, implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Remote Access | Managed Access Control Points (AC-17(3)):

- Route remote access through authorized and managed network access control points.

Remote Access | Privileged Commands and Access (AC-17(4)):

- Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and following agency needs.
- Document the rationale for remote access in the security plan for the system.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies shall implement the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may also be subject to additional Federal, State, and/or Inter-agency regulatory requirements. It is each agency's responsibility to research and implement additional controls needed to meet regulatory compliance requirements and expectations outside of the State of Wisconsin baseline of controls.

Remote Access | Disconnect or Disable Access (AC-17(9)):

- Provide the capability to disconnect or disable remote access to the system within an agency-defined time period.

102 Access Control for Wireless Access Standard

Purpose

This standard is intended to facilitate the attainment of the Access Control Policy and associated information technology (IT) security policy objectives.

This standard contains the minimum baseline controls that Executive Branch agencies shall implement; however, those agencies may also be required to implement controls outside of the scope of the controls listed in this document.

BASELINE CONTROLS

Wireless Access (AC-18):

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

Wireless Access | Authentication and Encryption (AC-18(1)):

- Protect wireless access to the system using authentication of users or devices and encryption.

Wireless Access | Disable Wireless Networking (AC-18(3)):

- Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

103 Access Control Standard for Mobile Device Security

Purpose

The Access Control for Mobile Device Security Standard provides documentation of the security requirements for the use of mobile device(s) (e.g., tablet, cell phone, PDA, smartwatch, or smart eyeglasses, etc.).

This standard contains the minimum baseline controls that Executive Branch agencies shall implement; however, those agencies may also be required to implement controls outside of the scope of the controls listed in this document.

BASELINE CONTROLS

Access Control for Mobile Devices (AC-19):

- Establish configuration requirements, connection requirements, and implementation guidance for agency-controlled mobile devices, to include when such devices are outside of controlled areas.
- Authorize the connection of mobile devices to agency systems.

Access Control for Mobile Devices | Full Device and Container Based-Encryption (AC-19(5)):

- Employ full-device or container-based encryption to protect the confidentiality and integrity of information on agency-defined mobile devices.

110 Security Awareness and Training Standard

Purpose

The purpose of the Security and Awareness Training Standard is to establish minimum training requirements supporting users who access and process Information residing on the State of Wisconsin information systems and its infrastructure.

This standard contains the minimum baseline controls that Executive Branch agencies shall implement; however, those agencies may also be required to implement controls outside of the scope of the controls listed in this document.

BASELINE CONTROLS

Policy and Procedures (AT-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
  - An awareness and training policy that:
    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
  - Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the awareness and training policy and procedures.
- Review and update the current awareness and training:
  - Policy on an agency-defined frequency.
  - Procedures on an agency-defined frequency.

Literacy Training and Awareness (AT-2):

- Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):
  - As part of initial training for new users and on an agency-defined frequency thereafter.
  - When required by system changes or following agency-defined events.
- Employ multiple techniques to increase the security and privacy awareness of system users. Techniques may include displaying posters, offering supplies inscribed with security and privacy reminders, displaying logon screen messages, generating email advisories or notices, and conducting awareness events.
- Update literacy training and awareness content on an agency-defined frequency and following agency-defined events.
- Incorporate lessons learned from internal or external security or privacy incidents into literacy training and awareness techniques.

Literacy Training and Awareness | Insider Threat (AT-2(2)):

- Provide literacy training on recognizing and reporting potential indicators of insider threat.

Literacy Training and Awareness | Social Engineering and Mining (AT-2(3)):

- Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

Role-Based Training (AT-3):

- Provide role-based security and privacy training to personnel with agency-defined roles and responsibilities:
  - Before authorizing access to the system, information, or performing assigned duties, and on an agency-defined frequency thereafter.
  - When required by system changes.
- Update role-based training content on an agency-defined frequency and following agency-defined events.
- Incorporate lessons learned from internal or external security or privacy incidents into role-based training.

Role-Based Training | Processing Personally Identifiable Information (AT-3(5)):

- Provide appropriate agency personnel or roles with initial training and training on an agency-defined frequency in the employment and operation of personally identifiable information processing and transparency controls.

Training Records (AT-4):

- Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training.
- Retain individual training records for five (5) years.

120 Audit and Accountability Standard

Purpose

The Audit and Accountability standard provides documentation of the requirements of the Audit and Accountability Policy, the Configuration Management Policy, the Maintenance Policy, and the System and Information and Integrity Policy.

This standard is divided into two sections of controls. **Section One** contains the minimum baseline controls that Executive Branch agencies shall implement. **Section Two** contains some of the common, regulatory controls agencies may be required to implement in addition to the baseline controls. Section Two is not all-inclusive. Each agency is responsible for identifying what other controls their agency may be required to implement beyond the scope of this standard.

SECTION ONE: BASELINE CONTROLS

Policy and Procedures (AU-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
    - An audit and accountability policy that:
        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
        - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
    - Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the audit and accountability policy and procedures.
- Review and update the current audit and accountability:
    - Policy on an agency-defined frequency.
    - Procedures on an agency-defined frequency.

Event Logging (AU-2):

- Identify the types of events that the system is capable of logging in support of the audit function.
- Coordinate the event logging function with other agency/organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged.
- Specify the event types for logging within the system. (Note: Appendix A includes security events that are recommended to be logged for all systems. The security events in Appendix A are not all-inclusive. There may be additional events the agency needs to consider, specific to its own operations, which are not included in Appendix A. Each agency shall identify what security events beyond those listed in Appendix A are necessary and appropriate in its environment.).
- Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents.
- Review and update the event types selected for logging on an agency-defined frequency.

Content of Audit Records (AU-3):

- Ensure that audit records contain information that establishes the following:
    - What type of event occurred.
    - When the event occurred.
    - Where the event occurred.
    - Source of the event.

  - Outcome of the event.
  - Identity of any individuals, subjects, or objects/entities associated with the event.

Content of Audit Records | Additional Audit Information (AU-3(1)):

- Generate audit records containing any additional information that the agency deems as necessary and appropriate (i.e., access control or flow control rules invoked and individual identities of group account users).

Content of Audit Records | Limit Personally Identifiable Information Elements (AU-3(3)):

- Limit personally identifiable information contained in audit records to elements identified in the privacy risk assessment.

Audit Log Storage Capacity (AU-4):

- Allocate audit log storage capacity to accommodate audit log retention requirements. Audit log retention requirements are defined in AU-11.

Response to Audit Logging Process Failures (AU-5):

- Alert appropriate, personnel (or roles) in as close to real-time as possible in the event of an audit logging process failure.
- Take the appropriate actions to address the alert and failure.

Audit Record Review, Analysis, and Reporting (AU-6):

- Review and analyze system audit records as close to real-time as possible for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity.
- Report findings to appropriate agency personnel or roles.
- Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Audit Record Review, Analysis, and Reporting | Automated Process Integration (AU-6(1)):

- Integrate audit record review, analysis, and reporting processes using automated mechanisms.

Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories (AU-6(3)):

- Analyze and correlate audit records across different repositories to gain situational awareness across all three levels of risk management (i.e., organizational level, mission/business process level, and information system level).

Audit Record Reduction and Report Generation (AU-7):

- Provide and implement an audit record reduction and report generation capability that:
  - Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents.
  - Does not alter the original content or time ordering of audit records.

Audit Record Reduction and Report Generation | Automatic Processing (AU-7(1)):

- Provide and implement the capability to process, sort, and search audit records for events of interest based on agency-defined fields within the audit records.

Time Stamps (AU-8):

- Use internal system clocks to generate time stamps for audit records.

- Record time stamps for audit records that are synchronized to the Department of Commerce (DOC) National Institute of Standards and Technology (NIST) Boulder Labs time source, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

Protection of Audit Information (AU-9):

- Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
- Alert appropriate agency personnel or roles upon detection of unauthorized access, modification, or deletion of audit information.

Protection of Audit Information | Access by Subset of Privileged Users (AU-9(4)):

- Authorize access to management of audit logging functionality to only those individuals/roles with a specific need or business justification for access to the records.

Audit Record Retention (AU-11):

- Retain audit records for a time period consistent with records retention policies as required by applicable state and federal laws to provide support for after-the-fact investigations of security incidents and to meet regulatory audit record retention requirements. Logs are to be maintained and readily available for a minimum of 90 days. Audit records are to be retained for one (1) year or longer, depending on regulatory requirements.

Audit Record Generation (AU-12):

- Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2.
- Allow limited personnel/roles to select the event types that are to be logged by specific components of the system.
- Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies shall implement the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may also be subject to additional Federal, State, and/or Inter-agency regulatory requirements. It is each agency's responsibility to research and implement additional controls needed to meet regulatory compliance requirements and expectations outside of the State of Wisconsin baseline of controls.

Response to Audit Logging Process Failures | Storage Capacity Warning (AU-5(1)):

- Provide a warning to appropriate agency personnel or roles within an agency-defined time period when allocated audit log storage volume reaches an agency-defined percentage of repository maximum audit log storage capacity.

Protection of Audit Information | Store on Separate Physical Systems or Components (AU-9(2)):

- Store audit records for an agency-defined frequency in a repository that is part of a physically different system or system component than the system or component being audited.

120 Audit and Accountability Standard Appendix A

Security events that are **recommended** to be logged for all systems include but are not limited to (AU-2):

1. The audit trail shall capture all successful login and logoff attempts.
2. The audit trail shall capture all unsuccessful login and authorization attempts.
3. The audit trail shall capture all identification and authentication attempts.
4. The audit trail shall capture all actions, connections and requests performed by privileged users (a user who, by virtue of function, and/or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator(s) and network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users).
5. The audit trail shall capture all actions, connections and requests performed by privileged functions.
6. The audit trail shall capture all changes to logical access control authorities (e.g., rights, permissions).
7. The audit trail shall capture all system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.
8. The audit trail shall capture the creation, modification, and deletion of objects including files, directories, and user accounts.
9. The audit trail shall capture the creation, modification and deletion of user accounts and group accounts.
10. The audit trail shall capture the creation, modification, and deletion of user account and group account privileges.
11. The audit trail shall capture: i) the date of the system event; ii) the time of the system event; iii) the type of system event initiated; and iv) the user account, system account, service, or process responsible for initiating the system event.
12. The audit trail shall capture system start-up and shutdown functions.
13. The audit trail shall capture modifications to administrator account(s) and administrator group account(s) including: i) escalation of user account privileges commensurate with administrator-equivalent account(s); and ii) adding or deleting users from the administrator group account(s).

120 Audit and Accountability Standard Appendix A (Continued)

Security events that are recommended to be logged for all systems include but are not limited to (AU-2):

14. The audit trail shall capture the enabling or disabling of audit report generation services.

15. The audit trail shall capture configuration changes made to the system (e.g., operating system, application, and database) that have relevance to information security.

16. The audit trail shall be protected from unauthorized access, use, deletion, or modification.

17. The audit trail shall be restricted to personnel routinely responsible for performing security audit functions.

130 Security Assessment and Authorization Standard

Purpose

The purpose of the Security Assessment and Authorization Standard is to establish a framework that assesses the State of Wisconsin information system security controls, provides for a Plan of Action and Milestones (POA&M) remediation effort, provides for continuous monitoring, system authorization, etc., and to ensure the Confidentiality, Integrity, and Availability (CIA) of the State of Wisconsin information systems, its environments, and its data.

This standard is divided into two sections of controls. **Section One** contains the minimum baseline controls that Executive Branch agencies shall implement. **Section Two** contains some of the common, regulatory controls agencies may be required to implement in addition to the baseline controls. Section Two is not all-inclusive. Each agency is responsible for identifying what other controls their agency may be required to implement beyond the scope of this standard.

SECTION ONE: BASELINE CONTROLS

Policy and Procedures (CA-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
  - An assessment, authorization, and monitoring policy that:
    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
  - Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures.
- Review and update the current assessment, authorization, and monitoring:
  - Policy on an agency-defined frequency.
  - Procedures on an agency-defined frequency.

Control Assessments (CA-2):

- Select the appropriate assessor or assessment team for the type of assessment to be conducted.
- Develop a control assessment plan that describes the scope of the assessment including:
  - Controls and control enhancements under assessment.
  - Assessment procedures to be used to determine control effectiveness.
  - Assessment environment, assessment team, and assessment roles and responsibilities.
- Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment.
- Assess the controls in the system and its environment of operation on an agency-defined frequency to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements.

- Produce a control assessment report that documents the results of the assessment.
- Provide the results of the control assessment to the appropriate agency personnel or roles.

Control Assessments | Independent Assessors (CA-2(1)):

- Employ independent assessors or assessment teams to conduct control assessments.

Information Exchange (CA-3):

- Approve and manage the exchange of information between the system and other systems using (one or more): interconnection security agreements, information exchange security agreements, memoranda of understanding or agreement, service level agreements, user agreements, nondisclosure agreements.
- Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of information communicated.
- Review and update the agreements on an agency-defined frequency.

Plan of Action and Milestones (CA-5):

- Develop a plan of action and milestones (POA&M) for the system to document the planned remediation actions of the agency to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system.
- Update existing plan of actions and milestones on an agency-defined frequency based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

Authorization (CA-6):

- Assign a senior official as the authorizing official for the system.
- Assign a senior official as the authorizing official for common controls available for inheritance by agency systems.
- Ensure that the authorizing official for the system, before commencing operations:
  - Accepts the use of common controls inherited by the system.
  - Authorizes the system to operate.
- Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by agency systems.
- Update the authorizations on an agency-defined frequency.

Continuous Monitoring (CA-7):

- Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the agency-level continuous monitoring strategy that includes:
  - Establishing the system-level metrics to be monitored.
  - Establishing the ongoing assessment of control effectiveness.
  - Ongoing control assessments in accordance with the continuous monitoring strategy.
  - Ongoing monitoring of system and metrics in accordance with the continuous monitoring strategy.
  - Correlation and analysis of information generated by control assessments and monitoring.
  - Response actions to address results of analysis of control assessment and monitoring information.
  - Reporting the security and privacy status of the system to the appropriate agency personnel or roles.

Continuous Monitoring | Independent Assessment (CA-7(1)):

- Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

Continuous Monitoring | Risk Monitoring (CA-7(4)):

- Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:
  - Effectiveness monitoring.
  - Compliance monitoring.
  - Change monitoring.

Internal System Connections (CA-9):

- Authorize internal connections of components to the system.
- Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated.
- Terminate internal system connections when no longer needed.
- Review on an agency-defined frequency the continued need for each internal connection.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies shall implement the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may also be subject to additional Federal, State, and/or Inter-agency regulatory requirements. It is each agency's responsibility to research and implement additional controls needed to meet regulatory compliance requirements and expectations outside of the State of Wisconsin baseline of controls.

Penetration Testing (CA-8):

- Conduct penetration testing on an agency-defined frequency on agency-defined systems or system components.

140 Configuration Management Standard

Purpose

The Configuration Management Standard provides documentation of the minimum requirements for secure and compliant configuration of the Enterprise IT systems and system environments.

Secure and compliant IT system configuration baselines shall align with one or more of the acceptable industry guidelines, a few of which are identified below. Exceptions, changes, or non-standard alterations to a secure and compliant configuration can be requested to meet a business or compliance need per the Enterprise Exception Procedure.

Industry Guidelines

- Center for Internet Security (CIS) Benchmarks
- Defense Information Systems Agency (DISA) Standard Technical Implementation Guidelines (STIG)
- National Institute of Science and Technology (NIST) National Checklist Program
- United States Government Configuration Baselines (USGCB)
- National Security Agency Security Configuration Guides
- International Organization for Standardization (ISO)

Primary Regulatory and Compliance Requirements (for Executive Branch Agencies)

- Centers for Medicare and Medicaid Services (CMS) - Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges (MARS-E)
- Criminal Justice Information Services (CJIS) Security Policy
- Family Educational Rights and Privacy Act (FERPA) Compliance
- Federal Information Security Management Act (FISMA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Internal Revenue Service (IRS) Publication 1075
- Payment Card Industry – Data Security Standard (PCI-DSS)
- Social Security Administration (SSA) Technical System Security Requirements
    - Wis. Stat. § 16.971

This standard is divided into two sections of controls. **Section One** contains the minimum baseline controls that Executive Branch agencies shall implement. **Section Two** contains some of the common regulatory controls agencies may be required to implement in addition to the baseline controls. Section Two is not all-inclusive. Each agency is responsible for identifying what other controls their agency may be required to implement beyond the scope of this standard.

SECTION ONE: BASELINE CONTROLS

Policy and Procedures (CM-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
    - A configuration management policy that:
        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
        - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

    - Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the configuration management policy and procedures.
- Review and update the current configuration management:
    - Policy on an agency-defined frequency.
    - Procedures on an agency-defined frequency.

Baseline Configuration (CM-2):

- Develop, document, and maintain under configuration control, a current baseline configuration of the system.
- Review and update the baseline configuration of the system:
    - On an agency-defined frequency.
    - When required due to system changes.
    - When system components are installed or upgraded.

Baseline Configuration | Automation Support for Accuracy and Currency (CM-2(2)):

- Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using automated mechanisms (i.e., configuration management tools, hardware, software, firmware inventory tools, or network management tools).

Baseline Configuration | Retention of Previous Configurations (CM-2(3)):

- Retain an agency-defined number of previous versions of baseline configurations of the system to support rollback.

Baseline Configuration | Configure Systems and Components for High-Risk Areas (CM-2(7)):

- Issue agency-defined systems or system components with agency-defined configurations to individuals traveling to locations that the agency deems to be of significant risk.
- Apply agency-defined controls to the systems or components when the individuals return from travel.

Configuration Change Control (CM-3):

- Determine and document the types of changes to the system that are configuration controlled.
- Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses.
- Document configuration change decisions associated with the system.
- Implement approved configuration-controlled changes to the system.
- Retain records of configuration-controlled changes to the system for the life of the system.
- Monitor and review activities associated with configuration-controlled changes to the system.
- Coordinate and provide oversight for configuration change control activities through a change control board that convenes on a frequent basis (defined by the agency).

Configuration Change Control | Testing, Validation, and Documentation of Changes (CM-3(2)):

- Test, validate, and document changes to the system before finalizing the implementation of the changes.

Configuration Change Control | Security and Privacy Representatives (CM-3(4)):

- Require security and privacy representatives to be members of the change control board.

Impact Analyses (CM-4):

- Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

Impact Analyses | Verification of Controls (CM-4(2)):

- After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome regarding meeting the security and privacy requirements for the system.

Access Restrictions for Change (CM-5):

- Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

Configuration Settings (CM-6):

- Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements.
- Implement the configuration settings.
- Identify, document, and approve the deviations from established configuration settings.
- Monitor and control changes to the configuration settings in accordance with State and agency policies and procedures.

Least Functionality (CM-7):

- Configure the system to provide only the missions, functions, or operations deemed essential by the agency.
- Prohibit or restrict the use of functions, ports, protocols, software, and/or services to only those individuals/groups who require it for their job duties.

Least Functionality | Periodic Review (CM-7(1)):

- Review the system on an agency-defined frequency to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services.
- Disable or remove the functions, ports protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

Least Functionality | Prevent Program Execution (CM-7(2)):

- Prevent program execution in accordance with policies, rules of behavior, and/or access agreements regarding software program usage and restrictions as well as the rules authorizing the terms and conditions of software program usage.

Least Functionality | Authorized Software (CM-7(5)):

- Identify the software programs authorized to execute on the system.
- Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system.
- Review and update the list of authorized software programs on an agency-defined frequency.

System Component Inventory (CM-8):

- Develop and document an inventory of system components that:
  - Accurately reflects the system.

  - Includes all components within the system.
  - Does not include duplicate accounting of components or components assigned to any other systems.
  - Is at the level of granularity deemed necessary for tracking and reporting.
  - Includes the necessary information to achieve effective system component accountability.
- Review and update the system component inventory on an agency-defined frequency.

System Component Inventory | Updates During Installation and Removal (CM-8(1)):

- Update the inventory of the system components as part of component installations, removals, and system updates.

System Component Inventory | Automated Unauthorized Component Detection (CM-8(3)):

- Detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms on an ongoing basis.
- Take appropriate actions when unauthorized components are detected by disabling network access by such components, isolating the components, and/or notifying the appropriate personnel.

Configuration Management Plan (CM-9):

- Develop, document, and implement a configuration management plan for the system that:
  - Addresses roles, responsibilities, and configuration management processes and procedures.
  - Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.
  - Defines the configuration items for the system and places the configuration items under configuration management.
  - Is reviewed and approved by designated agency personnel.
  - Protects the configuration management plan from unauthorized disclosure and modification.

Software Usage Restrictions (CM-10):

- Use software and associated documentation in accordance with contract agreements and copyright laws.
- Track the usage of software and associated documentation protected by quantity licenses to control copying and distribution.
- Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

User-Installed Software (CM-11):

- Establish policies for governing the installation of software by end users.
- Enforce software installation policies through agency-defined methods.
- Monitor policy compliance on an agency-defined frequency.

Information Location (CM-12):

- Identify and document the location of agency information and the specific system components on which the information is processed and stored.
- Identify and document the users who have access to the system and system components where the

information is processed and stored.

- Document changes to the location (i.e., system or system components) where the information is processed and stored.

Information Location | Automated Tools to Support Information Location (CM-12(1)):

- Use automated tools to identify agency-defined information by information type on agency-defined system components to ensure controls are in place to protect agency information and individual privacy.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies shall implement the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may also be subject to additional Federal, State, and/or Inter-agency regulatory requirements. It is each agency's responsibility to research and implement additional controls needed to meet regulatory compliance requirements and expectations outside of the State of Wisconsin baseline of controls.

Impact Analyses | Separate Test Environments (CM-4(1)):

- Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.

Access Restrictions for Change | Automated Access Enforcement and Audit Records (CM-5(1)):

- Enforce access restrictions using automated mechanisms.
- Automatically generate audit records of the enforcement actions.

Access Restrictions for Change | Privilege Limitation for Production and Operation (CM-5(5)):

- Limit privileges to change system components and system-related information within a production or operational environment.
- Review and reevaluate privileges on an agency-defined frequency.

Additional Documentation:

- DET Change Management Policy
- DET Change Management Procedure
- DET Pre-Approved Change List
- DET Communication Listservs
- DET Weekly OPCOM Change Planning and Coordination (CPAC) Reports

150 Contingency Planning Standard

Purpose

The purpose of the Contingency Planning Standard is to is to set forth requirements and expectations related to and supporting a resilient posture against unscheduled interruptions/downtime to the State of Wisconsin information systems and data, and to ensure that its staff and business partners are well-informed of their responsibilities when a disruption of business operations occurs and requires immediate action. Additionally, this standard provides requirements for the development of a contingency plan to restore an established level of service to State IT systems, system environments, and services as required by the Contingency Planning Policy and the Incident Response Policy.

This standard is divided into two sections of controls. **Section One** contains the minimum baseline controls that Executive Branch agencies shall implement. **Section Two** contains some of the common, regulatory controls agencies may be required to implement in addition to the baseline controls. Section Two is not all-inclusive. Each agency is responsible for identifying what other controls their agency may be required to implement beyond the scope of this standard.

SECTION ONE: BASELINE CONTROLS

Policy and Procedures (CP-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
    - A contingency planning policy that:
        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
        - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
    - Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the contingency planning policy and procedures.
- Review and update the current contingency planning:
    - Policy on an agency-defined frequency.
    - Procedures on an agency-defined frequency.

Contingency Plan (CP-2):

- Develop a contingency plan for the system that:
    - Identifies essential mission and business functions and associated contingency requirements.
    - Provides recovery objectives, restoration priorities, and metrics.
    - Addresses contingency roles, responsibilities, assigned individuals with contact information.
    - Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure.
    - Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented.
    - Addresses the sharing of contingency information.
    - Is reviewed and approved by designated agency personnel.
- Distribute copies of the contingency plan to key contingency personnel (identified by name

and/or by role) and organizational elements.

- Coordinate contingency planning activities with incident handling activities.
- Review the contingency plan for the system annually.
- Update the contingency plan to address changes to the agency, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.
- Communicate contingency plan changes to key contingency personnel (identified by name and/or by role) and organizational elements.
- Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training.
- Protect the contingency plan from unauthorized disclosure and modification.

Contingency Plan | Coordinate with Related Plans (CP-2(1)):

- Coordinate contingency plan development with organizational elements responsible for related plans.

Contingency Plan | Resume Mission and Business Functions (CP-2(3)):

- Plan for the resumption of all or essential mission and business functions within a defined time period of contingency plan activation.

Contingency Plan | Identify Critical Assets (CP-2(8)):

- Identify critical system assets supporting all or essential mission and business functions.

Contingency Training (CP-3):

- Provide contingency training to system users consistent with assigned roles and responsibilities:
  - Prior to assuming a contingency role or responsibility.
  - When required by system changes.
  - Annually thereafter.
- Review and update contingency training content annually and following agency-defined events (i.e., contingency plan testing, an actual contingency, assessment or audit findings, security or privacy incidents, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines).

Contingency Plan Testing (CP-4):

- Test the contingency plan for the system annually using tests (i.e., checklists, walk-through and tabletop exercises, simulations, comprehensive exercises) to determine the effectiveness of the plan and the readiness to execute the plan.
- Review the contingency plan test results.
- Initiate corrective actions, if needed.

Contingency Plan Testing | Coordinate with Related Plans (CP-4(1)):

- Coordinate contingency plan testing with organizational elements responsible for related plans.

Alternate Storage Site (CP-6):

- Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information.
- Ensure that the alternate storage site provides controls equivalent to that of the primary site.

Alternate Storage Site | Separation from Primary Site (CP-6(1)):

- Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

Alternate Storage Site | Accessibility (CP-6(3)):

- Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Alternate Processing Site (CP-7):

- Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of system operations for essential mission and business functions, within a time period consistent with recovery time and recovery point objectives, when the primary processing capabilities are unavailable.
- Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within an agency-defined time period for transfer and resumption.
- Provide controls at the alternate processing site that are equivalent to those at the primary site.

Alternate Processing Site | Separation from Primary Site (CP-7(1)):

- Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

Alternate Processing Site | Accessibility (CP-7(2)):

- Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Alternate Processing Site | Priority of Service (CP-7(3)):

- Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

Telecommunications Services (CP-8):

- Establish alternate telecommunications services, including necessary agreements to permit the resumption of system operations for essential mission and business functions within an agency-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Telecommunications Services | Priority of Service Provisions (CP-8(1)):

- Develop primary and alternate telecommunications service agreements that contain priority-or-service provisions in accordance with availability requirements (including recovery time objectives).

Telecommunications Services | Single Points of Failure (CP-8(2)):

- Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

System Backup (CP-9):

- Conduct backups of user-level information contained in system components on an agency-defined frequency consistent with recovery time and recovery point objectives.

- Conduct backups of system-level information contained in the system on an agency-defined frequency consistent with recovery time and recovery point objectives.
- Conduct backups of system documentation, including security- and privacy-related documentation on an agency-defined frequency consistent with recovery time and recovery point objectives.
- Protect the confidentiality, integrity, and availability of backup information.

System Backup | Testing for Reliability and Integrity (CP-9(1)):

- Test backup information on an agency-defined frequency to verify media reliability and information integrity.

System Backup | Cryptographic Protection (CP-9(8)):

- Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of backup information.

System Recovery and Reconstitution (CP-10):

- Provide for the recovery and reconstitution of the system to a known state, within an agency-defined time period consistent with recovery time and recovery point objectives, after a disruption, compromise, or failure.

System Recovery and Reconstitution | Transaction Recovery (CP-10(2)):

- Implement transaction recovery for systems that are transaction-based.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies shall implement the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may also be subject to additional Federal, State, and/or Inter-agency regulatory requirements. It is each agency’s responsibility to research and implement additional controls needed to meet regulatory compliance requirements and expectations outside of the State of Wisconsin baseline of controls.

Contingency Plan | Capacity Planning (CP-2(2)):

- Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

160 Identification and Authentication Standard

Purpose

The Identification and Authentication Standard provides documentation of the minimum requirements for verification of unique identity(s) and authentication of the identity of individuals, processes, and/or devices prior to accessing State IT systems, system environments, and services.

This standard is divided into two sections of controls. **Section One** contains the minimum baseline controls that Executive Branch agencies shall implement. **Section Two** contains some of the common, regulatory controls agencies may be required to implement in addition to the baseline controls. Section Two is not all-inclusive. Each agency is responsible for identifying what other controls their agency may be required to implement beyond the scope of this standard.

SECTION ONE: BASELINE CONTROLS

Policy and Procedures (IA-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
  - An identification and authentication policy that:
    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
  - Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the identification and authentication policy and procedures.
- Review and update the current identification and authentication:
  - Policy on an agency-defined frequency.
  - Procedures on an agency-defined frequency.

Identification and Authentication (Agency Users) (IA-2):

- Uniquely identify and authenticate agency users and associate that unique identification with processes acting on behalf of those users.

Identification and Authentication | Multi-factor Authentication to Privileged Accounts (IA-2(1)):

- Implement multi-factor authentication for access to privileged accounts.

Identification and Authentication (Agency Users) | Multi-factor Authentication to Non-Privileged Accounts (IA-2(2)):

- Implement multi-factor authentication for access to non-privileged accounts.

Identification and Authentication (Agency Users) | Access to Accounts – Replay Resistant (IA-2(8)):

- Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

Identification and Authentication (Agency Users) | Acceptance of PIV Credentials (IA-2(12)):

- Accept and electronically verify Personal Identity Verification-compliant credentials.

Device Identification and Authentication (IA-3):

- Uniquely identify and authenticate agency-defined devices and/or types of devices before establishing a connection (i.e., local, remote, or network connection).

Identifier Management (IA-4):

- Manage system identifiers by:
- Receiving authorization from designated agency personnel/roles to assign an individual, group, role, service, or device identifier.
- Selecting an identifier that identifies an individual, group, role, service, or device.
- Assigning the identifier to the intended individual, group, role, service, or device.
- Preventing reuse of identifiers for an agency-defined time period.

Note: NIST SP 800-63A addresses how applicants can prove their identities and become enrolled as valid subscribers within an identity system. It provides requirements by which applicants can both identity proof and enroll at one of three different levels of risk mitigation in both remote and physically present scenarios.

SP 800-63A sets requirements to achieve a given Identity Assurance Level (IAL). The three IALs reflect the options agencies may select from based on their risk profile and the potential harm caused by an attacker making a successful false claim of an identity. The IALs are as follows:

- IAL1: There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted or should be treated as such (including attributes a Credential Service Provider, or CSP, asserts to an RP).
- IAL2: Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically present identity proofing. Attributes can be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.
- IAL3: Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained CSP representative. As with IAL2, attributes could be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes. A CSP that supports IAL3 can support IAL1 and IAL2 identity attributes if the user consents.

For more information regarding Identifier Management, refer to NIST SP 800-63A, NIST SP 800-63C, and NIST SP 800-63-3.

Identifier Management | Identifier User Status (IA-4(4)):

- Manage individual identifiers by uniquely identifying each individual as agency-defined characteristic identifying individual status (Characteristics that identify the status of individuals include contractors, foreign nationals, and non-organizational users.).

Authenticator Management (IA-5):

- Manage system authentications by:
- Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator.
- Establishing initial authenticator content for any authenticators issued by the agency.

- Ensuring that authenticators have sufficient strength of mechanism for their intended use.
- Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators.
- Changing default authenticators prior to first use.
    - Changing or refreshing authenticators based on an agency-defined time period by authenticator type or when agency-defined events occur.
    - Protecting authenticator content from unauthorized disclosure and modification.
    - Requiring individuals to take, and have devices implement, specific controls to protect authenticators.
    - Changing authenticators for group or role accounts when membership to those accounts change.

Note: For services in which return visits are applicable, successful authentication provides reasonable risk-based assurances that the subscriber accessing the service today is the same as that which accessed the service previously. The robustness of this confidence is described by an Authenticator Assurance Level (AAL) categorization. NIST SP 800-63B addresses how an individual can securely authenticate to a CSP to access a digital service or set of digital services.

The three AALs define the subsets of options agencies can select based on their risk profile and the potential harm caused by an attacker taking control of an authenticator and accessing agencies' systems. The AALs are as follows:

- AAL1: AAL1 provides some assurance that the claimant controls an authenticator bound to the subscriber's account. AAL1 requires either single-factor or multi-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.
- AAL2: AAL2 provides high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required at AAL2 and above.
- AAL3: AAL3 provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication requires a hardware-based authenticator and an authenticator that provides verifier impersonation resistance; the same device may fulfill both these requirements. In order to authenticate at AAL3, claimants are required to prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required.

For more information regarding Authenticator Management, refer to NIST SP 800-63B, NIST SP 800-63C, and NIST SP 800-63-3. Baseline controls are at AAL1 while regulatory controls are at AAL2.

Authenticator Management | Password-Based Authentication (IA-5(1)):

- For password-based authentication:
    - Maintain a list of commonly used, expected, or compromised passwords and update the list annually and when passwords are suspected to have been compromised directly or indirectly.
    - Verify, when users create or update passwords, that the passwords are not found on the list of commonly used, expected, or compromised passwords.
    - Transmit passwords only over cryptographically protected channels.

- Store passwords using an approved salted key derivation function, preferably using a keyed hash.
- Require immediate selection of a new password upon account recovery.
- Allow user selection of long passwords and passphrases, including spaces and all printable characters, where applicable.
- Enforce the following settings when an agency-defined password policy is not configured to their own composition and complexity rules based on their regulatory directives:
    - Password length shall be a minimum of eight (8) characters for individual account access and a minimum of sixteen (16) characters for privileged administrative account access. The mainframe password length is limited to (8) characters for both privilege administrative and individual account access.
    - Passwords shall include three (3) of the following: uppercase letters, lowercase letters, numbers, special characters (e.g., !, @, #, $, etc.).
- Passwords shall not contain: your name, User ID, or simple patterns.

- Passwords are set to expire annually or on a more restrictive agency-defined frequency.
- Passwords shall not be re-used within 24 iterations.
- Access to accounts shall be locked after an agency-defined number of consecutive unsuccessful login attempts within an agency-defined time period.
- Temporary passwords provided for newly created or changed logons require an immediate change to a permanent password.
- Account holders shall maintain the confidentiality of passwords and any associated security questions/answers or other authentication information.
- Report any password abuse to the Enterprise Security via the ESD at (608) 264-9383 or ESDhelp@wisconsin.gov or Agency help desk.

Note: More restrictive password parameters may be implemented depending on the system/information being accessed. Those procedures should be documented accordingly. Exceptions at a lower requirement to this standard shall be requested via the Enterprise Exception Procedure and shall not be implemented without documented approval of the exception request.

Authenticator Management | Public Key-Based Authentication (IA-5(2)):

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

Authenticator Management | Protection of Authenticators (IA-5(6)):

- Protect authenticators commensurate with the security category of the information to which the authenticator permits access.

Authenticator Feedback (IA-6):

- Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals

Cryptographic Module Authentication (IA-7):

- Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

Identification and Authentication (Non-Agency Users) (IA-8):

- Uniquely identify and authenticate non-agency users or processes acting on behalf of non-agency users.

Identification and Authentication (Non-Agency Users) | Acceptance of PIV Credentials from Other Agencies (IA-8(1)):

- Accept and electronically verify Personal Identity Verification-compliant credentials from other agencies.

Identification and Authentication (Non-Agency Users) | Acceptance of External Authenticators (IA-8(2)):

- Accept only external authenticators that are NIST-compliant.
- Document and maintain a list of accepted external authenticators.

Identification and Authentication (Non-Agency Users) | Use of Defined Profiles (IA-8(4)):

- Conform to agency-defined identity management profiles for identity management.

Re-authentication (IA-11):

- Require users to re-authenticate when an agency-defined circumstance or situation occurs requiring re-authentication (i.e., when roles, authenticators, or credentials change, when security categories or systems change, when the execution of privileged functions occurs, after a fixed time period, or periodically).

Identity Proofing (IA-12):

- Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines.
- Resolve user identities to a unique individual.
- Collect, validate, and verify identity evidence.

Identity Proofing | Supervisor Authorization (IA-12(1)):

- Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.

Identity Proofing | Identity Evidence (IA-12(2)):

- Require evidence of individual identification be presented to the registration authority.

Identity Proofing | Identity Evidence Validation and Verification (IA-12(3)):

- Require that the presented identity evidence be validated and verified through an agency-defined method of validation and verification.

Identity Proofing | Address Confirmation (IA-12(5)):

- Require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the user's address (physical or digital) of record.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies shall implement the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may also be subject to additional Federal, State, and/or Inter-agency regulatory requirements. It is each agency's responsibility to research and implement additional controls needed to meet regulatory compliance requirements and expectations outside of the State of Wisconsin baseline of controls.

Identification and Authentication (Agency Users) | Individual Authentication with Group Authentication (IA-2(5)):

- When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

Authenticator Management | Change Authenticators Prior to Delivery (IA-5(5)):

- Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.

Authenticator Management | No Embedded Unencrypted Static Authenticators (IA-5(7)):

- Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

Compliance References

- NIST Special Publication 800-53, Revision 5
- NIST Special Publication 800-63A – Digital Identity Guidelines: Enrollment and Identity Proofing
- NIST Special Publication 800-63B – Digital Identity Guidelines: Authentication and Lifecycle Management
- NIST Special Publication 800-63C – Digital Identity Guidelines: Federation and Assertions
- NIST Special Publication 800-63-3 – Digital Identity Guidelines
- Internal Revenue Service (IRS) Publication 1075 (Rev. 11/21)
- DOJ FBI Criminal Justice Information Services Division – CJIS Security Policy (CJISSECPOL v6)
- NIST Special Publication 800-66r2 - Implementing the HIPAA Security Rule
- NIST Special Publication 800-122 - Protecting PII

170 Incident Response Standard

Purpose

The purpose of the Incident Response Standard is to set forth requirements and expectations related to preparation and handling information system security-related incidents including the monitoring, identification, reporting, response, handling of information system security-related incidents, and incident response plan testing and training, to ensure that State of Wisconsin staff and business partners are well-informed of their responsibilities when accessing and processing State of Wisconsin information systems, and its data.

This standard is divided into two sections of controls. **Section One** contains the minimum baseline controls that Executive Branch agencies shall implement. **Section Two** contains some of the common, regulatory controls agencies may be required to implement in addition to the baseline controls. Section Two is not all-inclusive. Each agency is responsible for identifying what other controls their agency may be required to implement beyond the scope of this standard.

SECTION ONE: BASELINE CONTROLS

Policy and Procedures (IR-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
    - An incident response policy that:
        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
        - Is consistent with applicable laws, executive orders, directives regulations, policies, standards, and guidelines.
    - Procedures to facilitate the implementation of the incident response policy and the associated incident response controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the incident response policy and procedures.
- Review and update the current incident response:
    - Policy on an agency-defined frequency.
    - Procedures on an agency-defined frequency.

Incident Response Training (IR-2):

- Provide incident response training to system users consistent with assigned roles and responsibilities:
    - Within an agency-defined time period of assuming an incident response role or responsibility or acquiring system access.
    - When required by system changes or reporting changes.
    - Annually thereafter
- Review and update the incident response training content based on agency requirements and following an agency-defined event.

Incident Response Training | Breach (IR-2(3)):

- Provide incident response training on how to identify and respond to a breach, including the agency’s process for reporting a breach.

Incident Response Testing (IR-3):

- Test the effectiveness of the incident response capability to identify potential weaknesses or deficiencies annually. A test can include various techniques, such as walkthroughs, tabletop exercises, simulations, and checklists.

Incident Response Testing | Coordination with Related Plans (IR-3(2)):

- Coordinate incident response testing with agency elements responsible for related plans.

Incident Handling (IR-4):

- Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection, and analysis, containment, eradication, and recovery.
- Coordinate incident handling activities with contingency planning activities.
- Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.
- Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the agency.

Incident Handling | Automated Incident Handling Processes (IR-4(1)):

- Support the incident handling process using automated mechanisms.

Incident Monitoring (IR-5):

- Track and document incidents.

Incident Reporting (IR-6):

- Require personnel to report suspected security, privacy, and supply chain incidents to the appropriate channels or personnel within an agency-defined time period.

Incident Reporting | Automated Reporting (IR-6(1)):

- Report incidents using automated mechanisms.

Incident Reporting | Supply Chain Coordination (IR-6(3)):

- Provide incident information to the provider of the product or service and other agencies involved in the supply chain or supply chain governance for systems or system components related to the incident.

Incident Response Assistance (IR-7):

- Provide an incident response support resource, integral to the agency incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

Incident Response Assistance | Automation Support for Availability of Information and Support (IR-7(1)):

- Increase the availability of incident response information and support using automated mechanisms.

Incident Response Plan (IR-8):

- Develop an incident response plan that:
    - Provides the agency with a roadmap for implementing its incident response capability.
    - Describes the structure and organization of the incident response capability.
    - Provides a high-level approach for how the incident response capability fits into the agency.
    - Meets the unique requirements for the agency, which relates to mission, size, structure, and functions.
    - Defines reportable incidents.
    - Provides metrics for measuring the incident response capability within the organization.
    - Defines the resource and management support needed to effectively maintain and mature an incident response capability.
    - Addresses the sharing of incident information.
    - Is reviewed and approved by designated agency personnel or roles on an annual basis.
    - Explicitly designates responsibility for incident response to agency-defined entities, personnel, or roles.
- Distribute copies of the incident response plan to appropriate personnel.
- Update the incident response plan to address system and agency changes or problems encountered during plan implementation, execution, or testing.
- Communicate incident response plan changes to appropriate personnel.
- Protect the incident response plan from unauthorized disclosure and modifications.

Incident Response Plan | Breaches (IR-8(1)):

- Include the following in the Incident Response Plan for breaches involving personally identifiable information:
    - A process to determine if notice to individuals or other organizations, including oversight organizations, is needed.
    - An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms.
    - Identification of applicable privacy requirements.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies shall implement the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may also be subject to additional Federal, State, and/or Inter-agency regulatory requirements. It is each agency's responsibility to research and implement additional controls needed to meet regulatory compliance requirements and expectations outside of the State of Wisconsin baseline of controls.

Incident Reporting | Vulnerabilities Related to Incidents (IR-6(2)):

- Report system vulnerabilities associated with reported incidents to the appropriate agency personnel or roles.

Incident Response Assistance | Coordination with External Providers (IR-7(2)):

- Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability.
- Identify agency incident response team members to the external providers.

Information Spillage Response (IR-9):

- Respond to information spills by:
    - Assigning designated incident response agency personnel with responsibility for responding to information spills.
    - Identifying the specific information involved in the system contamination.
    - Alerting designated agency officials of the information spill using a method of communication not associated with the spill.
    - Isolating the contaminated system or system component.
    - Eradicating the information from the contaminated system or component.
    - Identifying other systems or system components that may have been subsequently contaminated.
    - Performing additional actions as required by the agency.

180 System Maintenance Standard

Purpose

The purpose of the System Maintenance Standard is to set forth requirements and expectations related to, and supporting the scheduled maintenance, maintenance records, maintenance personnel, maintenance tools etc. of the State information system platforms, and to ensure that the State of Wisconsin IT staff and business partners are well-informed of their responsibilities when system maintenance is scheduled, implemented, and documented.

This standard is divided into two sections of controls. **Section One** contains the minimum baseline controls that Executive Branch agencies shall implement. **Section Two** contains some of the common, regulatory controls agencies may be required to implement in addition to the baseline controls. Section Two is not all-inclusive. Each agency is responsible for identifying what other controls their agency may be required to implement beyond the scope of this standard.

SECTION ONE: BASELINE CONTROLS

Policy and Procedures (MA-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
    - A maintenance policy that:
        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
        - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
    - Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the maintenance policy and procedures.
- Review and update the current maintenance:
    - Policy on an agency-defined frequency.
    - Procedures on an agency-defined frequency.

Controlled Maintenance (MA-2):

- Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and with consideration to incur the least amount of service interruption for the end-users, while being able to coordinate with venders and staff, as needed. Executive Branch Agency maintenance and freeze dates may be established to accommodate known fluctuations in staffing levels (e.g., holidays) or business needs (e.g., high processing times).
- Approve and monitor all maintenance activities, whether performed on site or remotely, and whether the system or system components are serviced onsite or removed to another location.
- Require that agency-defined personnel or roles explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement.
- Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: equipment that stored, processed, or transmitted data with the classification of sensitive or

above. This includes, but not limited to, any equipment that stored, processed, or transmitted FTI, Federal PII, State PII, and PHI.
- Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions.
- Document all maintenance services (e.g., via Cherwell).

Maintenance Tools (MA-3):

- Approve, control, and monitor the use of system maintenance tools.
- Review previously approved system maintenance tools annually to ensure the maintenance tools are not outdated, unsupported, irrelevant, or no-longer used.

Maintenance Tools | Inspect Tools (MA-3(1)):

- Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

Maintenance Tools | Inspect Media (MA-3(2)):

- Check media containing diagnostic and test programs for malicious code (e.g., virus, malware, trojans) before the media is utilized as part of maintenance services.

Maintenance Tools | Prevent Unauthorized Removal (MA-3(3)):

- Prevent the removal of maintenance equipment that contains State information by:
  - Verifying that there is no State information contained on the equipment.
  - Sanitizing or destroying the equipment.
  - Retaining the equipment within the secure area.
  - Obtaining an exception from certain personnel or defined personnel with certain roles, that explicitly authorizes the removal of equipment from the facility.

Non-local Maintenance (MA-4):

- Approve and monitor nonlocal maintenance and diagnostic activities.
- Allow the use of non-local maintenance and diagnostic tools consistent with agency policy and documented in the system security plan for the system if a system security plan is required.
- Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.
- Maintain records for nonlocal maintenance and diagnostic activities.
- Terminate session and network connections when nonlocal maintenance is completed.

Maintenance Personnel (MA-5):

- Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance personnel or organizations.
- Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations.
- Designate personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Timely Maintenance (MA-6):

- Obtain maintenance support and/or spare parts for State information systems and system environments within an agency-defined time period of failure. This can be based on the RTO within the disaster recovery or contingency plans.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies shall implement the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may also be subject to additional Federal, State, and/or Inter-agency regulatory requirements. It is each agency's responsibility to research and implement additional controls needed to meet regulatory compliance requirements and expectations outside of the State of Wisconsin baseline of controls.

Nonlocal Maintenance | Logging and Review (MA-4(1)):

- Log agency-defined audit events for nonlocal maintenance and diagnostic sessions.
- Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.

Nonlocal Maintenance | Cryptographic Protection (MA-4(6)):

- Implement cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.

Nonlocal Maintenance | Disconnect Verification (MA-4(7)):

- Verify session and network connection termination after the completion of non-local maintenance and diagnostic sessions.

Additional Documentation:

- DET Change Management Policy
- DET Change Management Procedure
- DET Pre-Approved Change List
- DET Communication Listservs
- DET Weekly OPCOM Change Planning and Coordination (CPAC) Reports

190 Media Protection Standard

Purpose

The purpose of the Media Protection standard is to set forth requirements and expectations related to and supporting the protection of physical and digital media containing non-public data including storage, marking, transport, sanitization, and access through the development of documentation to ensure that the State of Wisconsin staff and business partners are well-informed of their responsibilities when applying these principles within its information systems environment.

This standard is divided into two sections of controls. **Section One** contains the minimum baseline controls that Executive Branch agencies shall implement. **Section Two** contains some of the common, regulatory controls agencies may be required to implement in addition to the baseline controls. Section Two is not all-inclusive. Each agency is responsible for identifying what other controls their agency may be required to implement beyond the scope of this standard.

SECTION ONE: BASELINE CONTROLS

Policy and Procedures (MP-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
  - A media protection policy that:
    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
  - Procedures to facilitate the implementation of the media protection policy and the associated media protection controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the media protection policy and procedures.
- Review and update the current media protection:
  - Policy on an agency-defined frequency.
  - Procedures on an agency-defined frequency.

Media Access (MP-2):

- Restrict access to agency-defined types of digital and non-digital media to authorized individuals.

Media Marking (MP-3):

- Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.
- Exempt agency-defined types of system media from marking if the media remains within agency-defined controlled areas.

Media Storage (MP-4):

- Physically control and securely store agency-defined types of digital and non-digital media within agency-defined controlled areas. This includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the library, and maintaining accountability for stored media.
- Protect system media types defined in the above bullet, until the media is destroyed or sanitized

using approved equipment, techniques, and procedures.

Media Transport (MP-5):

- Protect and control agency-defined types of system media during transport outside of controlled areas using agency-defined controls.
- Maintain accountability for system media during the transport outside of controlled areas.
- Document activities associated with the transport of system media.
- Restrict the activities associated with the transport of system media to authorized personnel.

Media Sanitation (MP-6):

- Sanitize agency-defined system media prior to disposal, release out of agency control, or release for reuse using agency-defined sanitation techniques and procedures.
- Employ sanitation mechanisms with the strength and integrity commensurate with the security category or classification of the information.
- Follow the State of Wisconsin Records Retention and Disposal Policy, and applicable compliance regulations.

Media Sanitation | Review Approve, Track, Document, and Verify (MA-6(1))

- Agencies shall review, approve, track, document, and verify media sanitation and disposal actions.

Media Use (MP-7):

- Restrict or prohibit the use of personal media on agency systems or system components.
- Prohibit the use of portable storage devices in agency systems when such devices have no identifiable owner.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies shall implement the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may also be subject to additional Federal, State, and/or Inter-agency regulatory requirements. It is each agency's responsibility to research and implement additional controls needed to meet regulatory compliance requirements and expectations outside of the State of Wisconsin baseline of controls.

Media Sanitation | Equipment Testing (MP-6(2))

- Test sanitization equipment and procedures on an agency-defined frequency to ensure that the intended sanitization is being achieved.

191 Data Classification Standard

Purpose

The Data Classification Standard is intended to provide standardization for identification and classification of information assets, to facilitate the use of appropriate security, privacy, and compliance measures to protect the confidentiality, integrity, and availability of the information (data) and associated Information Technology (IT) resources according to its value and/or risk(s) to the agencies.

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact on the State if that data is disclosed, altered, or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate to safeguard that data. Executive Branch Agencies shall develop policies, procedures, or processes for their own State information and systems to protect State information, where applicable.

See the table below for one example of the confidentiality principle of data classification.

Classification	Adverse Business Impact	Description	Examples (not an exhaustive list)
Classified or Confidential	High	Any data where the unauthorized disclosure, alteration, loss, or destruction may cause personal or organizational financial loss or the unauthorized release of which would be a violation of a statute, act or law; constitute a violation of confidentiality agreed to as a condition of possessing or producing or transmitting data; cause significant reputational harm to the organization; or require the organization to self-report to the U.S. government and/or provide a public notice if the data is inappropriately accessed.	Subject to regulatory or compliance requirements (e.g., FTI, HIPAA, IRS, DMCA, PCI, PHI, PII, etc.). Data with contractual language requiring a confidential or high classification level of information/data. Information assets at this level shall limit access to authorized individuals only and shall employ encryption of data at rest, in use, and in transit (AC-21).
Restricted	Moderate	Any data, if released to unauthorized individuals, could have a mildly adverse impact on the organization's mission, safety, finances, or reputation. Data not specifically identified in another level is categorized as a "Moderate Risk".	Information assets at this level can be shared with individuals external to the agency and do not require encryption of data at rest or in use (AC-21).
Sensitive	Low	Any data where the unauthorized disclosure, alteration, loss, or destruction would have a low impact on the mission, safety, finances, or reputation of the organization.	Information assets at this level can be shared with individuals external to the agency and do not require encryption of data at rest, in use, or in transit (AC-21).

Public	Insignificant	Data that if breached owing to accidental or malicious activity would have an insignificant impact on the organization's activities and objectives.	Information assets at this level can be shared publicly and do not require encryption of data at rest, in use, or in transit (AC-21).

Compliance References

IRS Pub. 1075 (Rev 11/21)
NIST 800-53 Revision 5
NIST 800-60 Vol 1 and 2
FIPS 199

200 Physical and Environmental Protection Standard

Purpose

The purpose of the Physical and Environment Protection Standard is to set forth requirements and expectations related to and supporting the physical security of all State of Wisconsin facilities, technology, information systems and environments, and devices to ensure that the State of Wisconsin staff and business partners are well-informed of their responsibilities when accessing facilities and resources to store, process, and transmit State information.

This standard is divided into two sections of controls. **Section One** contains the minimum baseline controls that Executive Branch agencies shall implement. **Section Two** contains some of the common, regulatory controls agencies may be required to implement in addition to the baseline controls. Section Two is not all-inclusive. Each agency is responsible for identifying what other controls their agency may be required to implement beyond the scope of this standard.

SECTION ONE: BASELINE CONTROLS

Policy and Procedures (PE-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
  - A physical and environmental protection policy that:
    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
  - Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures.
- Review and update the current physical and environmental protection:
  - Policy on an agency-defined frequency.
  - Procedures on an agency-defined frequency.

Physical Security Access Authorizations (PE-2):

- Develop, approve and maintain a list of individuals with authorized access to the facility, including areas where system and system components reside.
- Issue authorization credentials for facility access and require individuals to wear identification badges.
- Review the access list detailing authorized facility access by individuals monthly.
- Remove individuals from the facility access list when access is no longer required.

Physical Access Control (PE-3):

- Enforce physical access authorizations at entry and exit points to the facility where the system resides by:
  - Verifying individual access authorizations before granting access to the facility.
  - Controlling ingress and egress to the facility using agency-defined physical access control systems, devices, or guards.

- Maintain physical access audit logs for agency-defined entry or exit points.
- Control access to areas within the facility designated as publicly accessible by implementing agency-defined physical access controls.
- Define circumstances when requiring visitor escorts and control of visitor activity.
- Secure keys, combinations, and other physical access devices.
- Inventory physical access devices annually.
- Change combinations and keys annually and/or when keys are lost, combinations are compromised, or when individuals processing keys or combinations are transferred or terminated.

Access Control for Transmission (PE-4):

- Control physical access to information system distribution and transmission lines within agency facilities using physical security safeguards.

Access Control for Output Devices (PE-5):

- Control physical access to output from output devices to prevent unauthorized individuals from obtaining the output (e.g., monitors, printers, scanners, audio devices, fax machines, and copiers).

Monitoring Physical Access (PE-6):

- Monitor physical access to the facility where systems reside to detect and respond to physical security incidents.
- Review physical access logs monthly and upon the occurrence of potential indications of events.
- Coordinate results of reviews and investigations with the agency incident response capability.

Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment (PE-6(1)):

- Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

Visitor Access Records (PE-8):

- Maintain visitor access records to the facility where the system resides for a minimum of 5 years.
- Review visitor access records monthly.
- Report anomalies in visitor access records to agency-defined personnel.

Visitor Access Records | Limit Personally Identifiable Information Elements (PE-8(3)):

- Limit personally identifiable information contained in visitor access records to elements identified in the privacy risk assessment.

Power Equipment and Cabling (PE-9):

- Protect power equipment and power cabling for the system from damage and destruction.

Emergency Shutoff (PE-10):

- Provide the capability of shutting off power to systems in emergency situations.
- Place emergency shutoff switches or devices within datacenters to facilitate access for authorized personnel.
- Protect emergency power shutoff capability from unauthorized activation.

Emergency Power (PE-11):

- Provide an uninterruptible power supply to facilitate an orderly shutdown of the system and/or transition of the system to long-term alternate power, in the event of a primary power source loss.

Emergency Lighting (PE-12):

- 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.

Fire Protection (PE-13):

- Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

Fire Protection | Detection Systems – Automatic Activation and Notification (PE-13(1))

- Employ fire detection systems that activate automatically and notify agency-defined personnel or roles and agency-defined emergency responders in the event of a fire.

Environmental Controls (PE-14):

- Maintain temperature and humidity controls in datacenters where State information systems and system environments reside.
- Monitor environmental control levels on an agency-defined frequency.

Water Damage Protection (PE-15):

- Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Delivery and Removal (PE-16):

- Authorize and control physical and environmental equipment that enters and exits secure areas in the facility.
- Maintain records of the system components.

Alternate Work Site (PE-17):

- Determine and document the agency permitted alternate work sites allowed for use by employees.
- Employ information system security and privacy controls at alternate work sites.
- Assess the effectiveness of security and privacy controls at alternate work sites.
- Provide a means for employees to communicate with information security and privacy personnel in case of security or privacy incidents.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies shall implement the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may also be subject to additional Federal, State, and/or Inter-agency regulatory requirements. It is each agency's responsibility to research and implement additional controls needed to meet regulatory compliance requirements and expectations outside of the State of Wisconsin baseline of controls.

Physical Access Authorizations | Access by Position or Role (PE-2(1)):

- Authorize physical access to the facility where the system resides based on position or role.

210 Security Planning Standard

Purpose

The purpose of the Security Planning standard is to set forth requirements and expectations related to, and supporting the development of privacy and security plans and related documentation to reflect the State of Wisconsin computing environments and to serve as a guide for protecting its information systems and data, to establish rules and behavior, and to ensure that staff and business partners are well-informed of their responsibilities when accessing and processing State of Wisconsin information systems data.

This standard contains the minimum baseline controls that Executive Branch agencies shall implement; however, those agencies may also be required to implement controls outside of the scope of the controls listed in this document.

BASELINE CONTROLS

Policy and Procedures (PL-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
  - A planning policy that:
    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
  - Procedures to facilitate the implementation of the planning policy and the associated planning controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the planning policy and procedures.
- Review and update the current planning:
  - Policy on an agency-defined frequency.
  - Procedures on an agency-defined frequency.

System Security and Privacy Plans (PL-2):

- Develop security and privacy plans for the system that:
  - Are consistent with the enterprise architecture.
  - Explicitly define the constituent system components.
  - Describe the operational context of the system in terms of mission and business processes.
  - Identify the individuals that fulfill system roles and responsibilities.
  - Identify the information types processed, stored, and transmitted by the system.
  - Provide the security categorization of the system, including supporting rationale.
  - Describe any specific threats to the system that are of concern to the agency.
  - Provide the results of a privacy risk assessment for systems processing personally identifiable information.
  - Describe the operational environment for the system and any dependencies on or connections to other systems or system components.
  - Provide an overview of the security and privacy requirements for the system.
  - Identify any relevant control baselines or overlays, if applicable.
  - Describe the controls in place or planned for meeting the security and privacy

requirements, including a rationale for any tailoring decisions.
  - Include risk determinations for security and privacy architecture and design decisions.
  - Include security- and privacy-related activities affecting the system that require planning and coordination with authorized agency personnel.
  - Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.
- Distribute copies of the plans and communicate subsequent changes to the plans to authorized agency personnel.
- Review the plans on an agency-defined frequency.
- Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments.
- Protect the plans from unauthorized disclosure and modification.

Rules of Behavior (PL-4):

- Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy (e.g., Acceptable Use Agreement).
- Receive a documented acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system.
- Review and update the rules of behavior on an agency-defined frequency.
- Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules are revised or updated.

Rules of Behavior | Social Media and External Site/Application Usage Restrictions (PL-4(1)):

- Include in the rules of behavior, restrictions on:
  - Use of social media, social networking sites, and external sites/applications.
  - Posting agency information on public websites.
  - Use of agency-provided identities (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

Security and Privacy Architectures (PL-8):

- Develop security and privacy architectures for the system that:
  - Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of agency information.
  - Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals.
  - Describe how the architectures are integrated into and support the enterprise architecture.
  - Describe any assumptions about, and dependencies on, external systems and services.
- Review and update the architecture annually to reflect changes in the enterprise architecture.
- Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, agency procedures, and procurements and acquisitions.

Central Management (PL-9):

- Centrally manage agency-defined controls and related processes.

Baseline Selection (PL-10):

- Select a control baseline for the system.

Baseline Tailoring (PL-11):

- Tailor the selected control baseline by applying specified tailoring actions.

220 Personnel Security Standard

Purpose

The Personnel Security standard provides documentation of the requirements to achieve compliance with the Personnel Security Policy and other applicable policies, procedures, and/or standards. This standard is applicable to all Executive Branch agency employees, interns, contractors, and/or vendors with access to State IT systems and system environments.

This standard contains the minimum baseline controls that Executive Branch agencies shall implement; however, those agencies may also be required to implement controls outside of the scope of the controls listed in this document.

BASELINE CONTROLS

Policy and Procedures (PS-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
- A personnel security policy that:
    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
- Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the personnel security policy and procedures.
- Review and update the current personnel security:
- Policy on an agency-defined frequency.
- Procedures on an agency-defined frequency.

Position Risk Designation (PS-2):

- Follow agency policies, procedures, and standards for assigning risk (or classification) and hiring employees, interns, and contractors.

Personnel Screening (PS-3):

- All State employees, interns, and contractors must have personnel (citizen/residency reference checks) and security (background checks) screenings prior to employment.
- Individuals who work at consolidated datacenters must have an FBI fingerprint background check initiated prior to accessing areas with sensitive or confidential areas.
- Security background checks are required at a minimum of every 5 years.

Personnel Termination (PS-4):

- Upon termination of individual employment:
    - Disable system access within an agency-defined time period.
    - Terminate or revoke any authenticators or credentials with the individual.
    - Conduct exit interviews, when applicable.
    - Retrieve all security-related organizational system-related property.
    - Retain access to agency information and systems formerly controlled by the terminated

individual.

Personnel Transfer (PS-5):

- Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the agency.
- Initiate agency-defined transfer or reassignment actions within an agency-defined period of time following the formal transfer.
- Modify access authorizations as needed to correspond with any changes in operational needs due to reassignment or transfer.
- Notify agency personnel or roles within an agency-defined time period.

Access Agreements (PS-6):

- Develop and document access agreements for agency systems.
- Review and update access agreements on an agency-defined frequency.
- Verify that individuals requiring access to agency information and systems:
  - Sign appropriate access agreements prior to being granted access.
  - Re-sign access agreements to maintain access to agency systems when agreements have been updated or required by an agency-defined frequency.

External Personnel Security (PS-7):

- Establish personnel security requirements, including security roles and responsibilities for external providers.
- Require external providers to comply with personnel security policies and procedures established by the agency.
- Document personnel security requirements.
- Require external providers to notify agency personnel or roles of any personnel transfers or terminations of external personnel who possess State information (including credentials/badges) or who have system privileges within an agency-defined time period.
- Monitor provider compliance with personnel security requirements.

Personnel Sanctions (PS-8):

- Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures.
- Notify designated agency personnel within an agency-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Position Descriptions (PS-9):

- Incorporate security and privacy roles and responsibilities into agency position descriptions.

230 Risk Assessment Standard

Purpose

The purpose of the Risk Assessment standard is to set forth requirements and expectations related to, and supporting Information Technology (IT) and Information Systems (IS) risk assessments, criticality analysis, security categorization of data, risk response (e.g., POAM remediation), vulnerability monitoring and scanning, etc. to identify the risk posture as part of the risk management framework process for the State of Wisconsin computing environments including its information systems and data. Various risk assessment types and strategies are used to address risk assessment, risk management, and risk mitigation/acceptance for State information and IT systems.

This standard contains the minimum baseline controls that Executive Branch agencies shall implement; however, those agencies may also be required to implement controls outside of the scope of the controls listed in this document.

BASELINE CONTROLS

Policy and Procedures (RA-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
  - A risk assessment policy that:
    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
  - Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the risk assessment policy and procedures.
- Review and update the current risk assessment:
  - Policy on an agency-defined frequency.
  - Procedures on an agency-defined frequency.

Security Categorization (RA-2):

- Categorize the systems and information it processes, stores, and transmits.
- Document the security categorization results, including supporting rationale, in the security plan for system.
- Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

Note: Categorization is not the same as Classification. Categorization identifies the type of data (e.g., FTI, PHI, Federal PII, HIPAA) where Classification is the higher tier of several categories. Using the example, the classification based on Federal guidance would be Sensitive But Unclassified (SBU) or Controlled Unclassified Information (CUI) under NIST SP 800-171 Rev. 2. Low, Moderate, and High controls are based on potential impact and selected to reduce the potential impact unless it is determined the likelihood of the potential impact is minimized. Federal security categories can be found in NIST SP 800-60 Vol. 1 and 2, on the Federal Register, or on some Federal agency websites.

Risk Assessment (RA-3):

- Conduct a risk assessment, including:
    - Identifying threats to and vulnerabilities in the system.
    - Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information the system processes, stores, or transmits, and any related information.
    - Determining the likelihood and impact of adverse effects on individuals arising from the processing of personal identifiable information (PII).
- Integrate risk assessment results and risk management decisions from the agency and mission or business process perspectives with system-level risk assessments.
- Document risk assessment results in security and privacy plans and risk assessment plans.
- Review risk assessment results on an agency-defined frequency.
- Disseminate risk assessment results to agency-defined personnel or roles.
- Update the risk assessment on an agency-defined frequency or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

Risk Assessment | Supply Chain Risk Assessment (RA-3(1)):

- Assess supply chain risks associated with agency-defined systems, system components, and system services.
- Update the supply chain risks assessment on an agency-defined frequency, when there are significant changes to the relevant supply chain, or when changes to the system, environments of operations, or other conditions may necessitate a change in the supply chain.

Vulnerability Monitoring and Scanning (RA-5):

- Monitor and scan for vulnerabilities in the system and hosted applications on an agency-defined frequency and when new vulnerabilities potentially affecting the system are identified and reported.
- Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    - Enumerating platforms, software flaws, and improper configurations
    - Formatting checklists and test procedures
    - Measuring vulnerability impact
- Analyze vulnerability scan reports and results from vulnerability monitoring.
- Remediate legitimate vulnerabilities in accordance with an agency assessment of risk.
- Share information obtained from the vulnerability monitoring process and control assessments with agency-defined personnel or roles to help eliminate similar vulnerabilities in other systems.
- Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned (RA-5(2)):

- Update the system vulnerabilities to be scanned on an agency-defined frequency, prior to a new scan, and when new vulnerabilities are identified and reported.

Vulnerability Monitoring and Scanning | Privileged Access (RA-5(5)):

- Implement appropriate privileged access authorization to system components for vulnerability scanning activities.

Vulnerability Monitoring and Scanning | Public Disclosure Program (RA-5(11)):

- Establish a public reporting channel for receiving reports of vulnerabilities in agency systems and system components.

Risk Response (RA-7):

- Respond to findings from security and privacy assessments, monitoring, and audits in accordance with agency risk tolerances.

Privacy Impact Assessments (RA-8):

- Conduct privacy impact assessments for systems, programs, or other activities before:
    - Developing or procuring information technology that processes personally identifiable information.
    - Initiating a new collection of personally identifiable information that:
        - Will be processed using information technology.

Criticality Analysis (RA-9):

- Identify critical system components and functions by performing a criticality analysis for agency-defined systems, system components, and system services. For example, critical systems and components can be documented in contingency plans, system security plans, asset databases (e.g., CMDB), or architecture diagrams.

240 System and Services Acquisition Standard

Purpose

The purpose of the System (assets) and Services Acquisition standard is to set forth requirements and expectations related to and supporting the roadmap for a standardized system and service acquisition process through the development of documentation and other essential related activities, to be adopted and implemented ensuring consistent alignment with the protection of privacy and security best practices.

This standard is divided into two sections of controls. **Section One** contains the minimum baseline controls that Executive Branch agencies shall implement. **Section Two** contains some of the common, regulatory controls agencies may be required to implement in addition to the baseline controls. Section Two is not all-inclusive. Each agency is responsible for identifying what other controls their agency may be required to implement beyond the scope of this standard.

SECTION ONE: BASELINE CONTROLS

Policy and Procedures (SA-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
    - A system and services acquisition policy that:
        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
        - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
    - Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures.
- Review and update the current system and services acquisition:
    - Policy on an agency-defined frequency.
    - Procedures on an agency-defined frequency.

Allocation of Resources (SA-2):

- Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning.
- Determine, document, and allocate the resources and funding to protect the system or system service as part of the organizational capital planning and investment control process.

  Note: Executive Branch agencies are required to follow Statewide IT planning, Annual Strategic IT Planning and Large, High Risk IT Project Reporting. See the following website for additional documentation: https://detcc.wi.gov/Pages/Strategic_IT_Planning.aspx.

System Development Life Cycle (SA-3):

- Acquire, develop, and manage the system using a system development life cycle process that incorporates information security and privacy considerations.
- Define and document information security and privacy roles and responsibilities throughout the system development life cycle.
- Identify individuals having information security and privacy roles and responsibilities.
- Integrate agency information security and privacy risk management process into the system

development life cycle activities.

Acquisition Process (SA-4):

- Include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the system, system component, or system services:
    - Security and privacy functional requirements
    - Strength of mechanism requirements
    - Security and privacy assurance requirements
    - Controls needed to satisfy the security and privacy requirements
    - Security and privacy documentation requirements
    - Requirements for protecting security and privacy documentation
    - Description of the system development environment and environment in which the system is intended to operate
    - Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management
    - Acceptance criteria

Acquisition Process | Functional Properties of Controls (SA-4(1)):

- Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

Acquisition Process | Design and Implementation of Information for Controls (SA-4(2)):

- Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes (one or more): security-relevant external system interfaces, high-level design; low-level design; source code or hardware schematics.

Acquisition Process | Function, Ports, Protocols, and Services in Use (SA-4(9)):

- Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for agency use.

Acquisition Process | Use of Approved PIV Products (SA-4(10)):

- Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within the agency systems.

System Documentation (SA-5):

- Obtain or develop administrator documentation for the system, system components, or system services that describes:
    - Secure configuration, installation, and operation of the system components, or services.
    - Effective use and maintenance of security and privacy functions and mechanisms.
    - Known vulnerabilities regarding configuration and use of administrative or privileged functions.
- Obtain or develop user documentation for the system, system component, or system services that describes:
    - User-accessible security and privacy functions and mechanisms on how to effectively use those functions and mechanisms.
    - Methods for user interaction, which enable individuals to use the system, component, or service in a more secure manner and protect individual privacy.

    - User responsibilities in maintaining the security of the system, component, or service and privacy of individuals.
- Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take agency-defined actions in response.
- Distribute documentation to the appropriate agency personnel or roles.

Security and Privacy Engineering Principles (SA-8):

- Apply system security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components.

Security and Privacy Engineering Principles | Minimization (SA-8(33)):

- Implement the privacy principle of minimization using agency-defined processes. The principle of minimization states that organizations should only process personally identifiable information that is directly relevant and necessary to accomplish an authorized purpose and should only maintain personally identifiable information for as long as necessary to accomplish the purpose.

External System Services (SA-9):

- Require providers of external system services comply with agency security and privacy requirements and employ agency-defined controls.
- Define and document agency oversite and user roles and responsibilities regarding external system services.
- Employ processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis.

External System Services | Identification of Functions, Ports, Protocols, and Services (SA-9(2)):

- Require providers of agency-defined external system services to identify the functions, ports, protocols, and other services required for the use of such services.

Developer Configuration Management (SA-10):

- Require the developer of the system, system component, or system service to:
    - Perform configuration management during system, component, or service: (one or more) design; development; implementation; operation; disposal.
    - Document, manage, and control the integrity of changes to agency-defined configuration items under configuration management.
    - Implement only agency-approved changes to the system, component, or service.
    - Document approved changes to the system, component, or service and the potential security impacts of such changes.
    - Track security flaws and flaw resolution within the system, component, or service and report findings to designated agency personnel or roles.

Developer Testing and Evaluation (SA-11):

- Require the developer of the information system, system component, or system service, at all post-design stages of the system development life cycle, to:
    - Develop and implement a plan for ongoing security and privacy assessments.
    - Perform testing/evaluation on an agency-defined frequency.
    - Produce evidence of the execution of the assessment plan and the results of the testing and

evaluation.
  - Implement variable flaw remediation process.
  - Correct flaws identified during security testing and evaluation.

Development Process, Standards, and Tools (SA-15):

- Require the developer of the system, system component, or system service to follow a documented development process that:
  - Explicitly addresses security and privacy requirements.
  - Identifies the standards and tools used in the development process.
  - Documents the specific tool options and tool configurations used in the development process.
  - Documents, manages, and ensures the integrity of changes to the process and/or tools used in development.
- Review the development process, standards, tools, tool options, and tool configurations on an agency-defined frequency to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the agency's security and privacy requirements.

Development Process, Standards, and Tools | Criticality Analysis (SA-15(3)):

- Require the developer of the system, system component, or system service to perform a criticality analysis:
  - At agency-defined decision points in the system development life cycle.
  - At agency-defined breadth and depth of criticality analysis level of rigor.

Unsupported System Components (SA-22)

- Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.
- Provide options for alternative sources for continued support of unsupported components.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies shall implement the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may also be subject to additional Federal, State, and/or Inter-agency regulatory requirements. It is each agency's responsibility to research and implement additional controls needed to meet regulatory compliance requirements and expectations outside of the State of Wisconsin baseline of controls.

Acquisition Process | Continuous Monitoring Plan for Controls (SA-4(8)):

- Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of the control effectiveness that is consistent with the continuous monitoring program of the agency.

External System Services | Risk Assessments and Agency Approvals (SA-9(1)):

- Conduct an agency assessment of risk prior to the acquisition or outsourcing of information security services.
- Verify that the acquisition or outsourcing of dedicated information security services is approved by the appropriate agency personnel or roles.

External System Services | Processing, Storage, and Service Location (SA-9(5)):

- Restrict the location of information processing, information or data, or system services to an agency-defined location based on agency-defined requirements or conditions.

Developer Configuration Management | Software and Firmware Integrity Verification (SA-10(1)):

- Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components.

Developer Testing and Evaluation | Static Code Analysis (SA-11(1)):

- Require the developer of the system, system component, or system services to employ static code analysis tools to identify common flaws and document the results of the analysis.

250 System and Communication Protection Standard

Purpose

The purpose of the System and Communications Protection Standard is to set forth requirements and expectations through the development of documentation related to and supporting effective security measures to provide protection of the State of Wisconsin information systems and data to meet all regulatory compliance requirements and expectations.

This standard is divided into two sections of controls. **Section One** contains the minimum baseline controls that Executive Branch agencies shall implement. **Section Two** contains some of the common, regulatory controls agencies may be required to implement in addition to the baseline controls. Section Two is not all-inclusive. Each agency is responsible for identifying what other controls their agency may be required to implement beyond the scope of this standard.

SECTION ONE: BASELINE CONTROLS

Policy and Procedures (SC-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
  - A system and communications protection policy that:
    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
  - Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the system and communications protection policy and procedures.
- Review and update the current system and communications protection:
  - Policy on an agency-defined frequency.
  - Procedures on an agency-defined frequency.

Separation of System and User Functionality (SC-2):

- Separate user functionality, including user interface services, from system management functionality. System management functionality includes functions that are necessary to administer databases, network components, workstations, or servers.

Information in Shared System Resources (SC-4):

- Prevent unauthorized and unintended information transfer via shared system resources.

Denial of Service Protection (SC-5):

- Protect against or limit the effects of denial-of-service events.
- Employ controls to achieve the denial-of-service objective.

Boundary Protection (SC-7):

- Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system.

- Implement subnetworks for publicly assessable system components that are physically and/or logically separated from internal agency networks.
- Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with agency security and privacy architecture.

Boundary Protection | Access Points (SC-7(3)):

- Limit the number of external network connections to the system to facilitate monitoring of inbound and outbound communications traffic.

Boundary Protection | External Telecommunications Services (SC-7(4)):

- Implement a managed interface for each external telecommunication service.
- Establish a traffic flow policy for each managed interface.
- Protect the confidentiality and integrity of the information being transmitted across each interface.
- Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need.
- Review exceptions to the traffic flow policy on an agency-defined frequency and remove exceptions that are no longer supported by an explicit mission or business need.
- Prevent unauthorized exchange of control plane traffic with external networks.
- Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks.
- Filter unauthorized control plane traffic from external networks.

Boundary Protection | Deny by Default – Allow by Exception (SC-7(5)):

- Deny network communications traffic by default and allow network communications traffic by exception at managed interfaces.

Boundary Protection | Prevent Split Tunneling for Remote Devices (SC-7(7)):

- Prevent split tunneling for remote devices connecting to systems unless the split tunnel is securely provisioned using agency-defined safeguards.

Boundary Protection | Route Traffic to Authenticated Proxy Services (SC-7(8)):

- Route agency-defined internal communications traffic to agency-defined external networks through authenticated proxy servers at managed interfaces.

Boundary Protection | Personally Identifiable Information (SC-7(24)):

- For systems that process personally identifiable information:
    - Apply agency-defined processing rules to data elements of personally identifiable information.
    - Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system.
    - Document each processing exception.
    - Review and remove exceptions that are no longer supported.

Transmission Confidentiality and Integrity (SC-8):

- Protect the confidentiality and integrity of transmitted information.

Transmission Confidentiality and Integrity | Cryptographic Protection (SC-8(1)):

- Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission.

Network Disconnect (SC-10):

- Terminate the network connection associated with a communications session at the end of the session or after 30 minutes of inactivity.

Cryptographic Key Establishment and Management (SC-12):

- Establish and manage cryptographic keys when cryptography is employed within the system in accordance with agency-defined key management requirements (e.g., key generation, distribution, storage, access, and destruction).

Cryptographic Protection (SC-13):

- Determine agency-defined cryptographic uses.
- Implement the agency-defined types of cryptography required for each specific cryptographic use.

Collaborative Computing Devices and Applications (SC-15):

- Prohibit remote activation of collaborative computing devices and applications.
- Provide an explicit indication of use to users physically present at the device.

Public Key Infrastructure Certificates (SC-17):

- Issue public key certificates under an appropriate certificate policy or obtain public key certificates from an approved service provider.
- Include only approved trust anchors in trust stores or certificate stores managed by the agency.

Mobile Code (SC-18):

- Define acceptable and unacceptable mobile code and mobile code technologies.
- Authorize, monitor, and control the use of mobile code and mobile code technologies within the system.

Secure Name/Address Resolution Service (Authoritative Source) (SC-20):

- Provide additional data origin authentication and integrity verification artifacts along with authoritative name resolution data the system returns in response to external name/address resolution queries.
- Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains; when operating as a part of a distributed, hierarchical namespace.

Secure Name/Address Resolution Service (Recursive or Caching Resolver) (SC-21):

- Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Architecture and Provisioning for Name/Address Resolution Service (SC-22):

- Ensure the systems that collectively provide name/address resolution service for an agency are fault-tolerant and implement internal and external role separation.

Session Authenticity (SC-23):

- Protect the authenticity of communication sessions.

Protection of Information at Rest (SC-28):

- Protect the confidentiality and integrity of agency-defined information at rest.

Protection of Information at Rest | Cryptographic Protection (SC-28(1)):

- Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest on agency-defined system components or media.

Process Isolation (SC-39):

- Maintain a separate execution domain for each executing system process.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies shall implement the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may also be subject to additional Federal, State, and/or Inter-agency regulatory requirements. It is each agency's responsibility to research and implement additional controls needed to meet regulatory compliance requirements and expectations outside of the State of Wisconsin baseline of controls.

Separation of System and User Functionality | Interfaces for Non-Privileged Users (SC-2(1)):

- Prevent the presentation of system management functionality at interfaces to non-privileged users.

Resource Availability (SC-6):

- Protect the availability of resources by allocating agency-defined resources by priority, quota, or agency-defined controls.

Boundary Protection | Restrict Incoming Communications Traffic (SC-7(11)):

- Only allow incoming communications from agency-defined authorized sources to be routed to agency-defined authorized destinations.

Boundary Protection | Host-Based Protection (SC-7(12)):

- Implement host-based boundary protection mechanisms at agency-defined system components.

Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components (SC-7(13)):

- Isolate agency-defined information security tools, mechanisms, and support components from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

Boundary Protection | Fail Secure (SC-7(18)):

- Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.

Transmission Confidentiality and Integrity | Pre- and Post-Transmission Handling (SC-8(2)):

- Maintain the confidentiality and/or integrity of information during preparation for transmission and during reception.

Cryptographic Key Establishment and Management | Symmetric Keys (SC-12(2)):

- Produce, control, and distribute symmetric cryptographic keys using NIST FIPS-validated or NSA-approved key management technology and process.

Cryptographic Key Establishment and Management | Asymmetric Keys (SC-12(3)):

- Produce, control, and distribute asymmetric cryptographic keys using one of the following: NSA-approved key management technology and processes; prepositioned keying material; DoD-approved or DoD-issued Medium Assurance PKI certificates; DoD-approved or DoD-issued Medium Hardware Assurance PKI certificates and hardware security tokens that protect the user's private key; certificates issued in accordance with agency-defined requirements.

Mobile Code | Identify Unacceptable Code and Take Corrective Action (SC-18(1)):

- Identify agency-defined unacceptable mobile code and take corrective actions.

Mobile Code | Acquisition, Development, and Use (SC-18(2)):

- Verify that the acquisition, development, and use of mobile code to be deployed in the system meets agency-defined mobile code requirements.

Session Authenticity | Invalidate Session Identifiers at Logout (SC-23(1)):

- Invalidate session identifiers upon user logout or other session termination.

Session Authenticity | Unique System-Generated Session Identifiers (SC-23(3)):

- Generate a unique session identifier for each session with agency-defined randomness requirements and recognize only session identifiers that are system-generated.

System Partitioning (SC-32):

- Partition the system into agency-defined system components residing in separate physical or logical domains or environments based on agency-defined circumstances for physical or logical separation of components.

260 System and Information Integrity Standard

Purpose

The purpose of the System and Information Integrity standard is to set forth requirements and expectations through the development of documentation related to, and supporting the protection of the State of Wisconsin information systems and data against threats and vulnerabilities that may compromise the integrity of its information systems and data.

This standard is divided into two sections of controls. **Section One** contains the minimum baseline controls that Executive Branch agencies shall implement. **Section Two** contains some of the common, regulatory controls agencies may be required to implement in addition to the baseline controls. Section Two is not all-inclusive. Each agency is responsible for identifying what other controls their agency may be required to implement beyond the scope of this standard.

SECTION ONE: BASELINE CONTROLS

Policy and Procedures (SI-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
    - A system and information integrity policy that:
        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
        - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
    - Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the system and information integrity policy and procedures.
- Review and update the current system and information integrity:
    - Policy on an agency-defined frequency.
    - Procedures on an agency-defined frequency.

Flaw Remediation (SI-2):

- Identify, report, and correct system flaws.
- Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
- Install security-relevant software and firmware updates within agency-defined time periods of the release of the updates.
- Incorporate flaw remediation into the agency configuration management process.
- Note: Executive branch agencies are responsible for systems and/or software that no longer have security patches available or have business needs that conflict with patching requirements. These systems and/or software are required to follow the DOA/DET Exception Process

Flaw Remediation | Automated Flaw Remediation Status (SI-2(2)):

- Determine if system components have applicable security-relevant software and firmware updates installed using automated mechanisms on an agency-defined frequency.

Malicious Code Protection (SI-3):

- Implement signature-based and/or non-signature-based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.
- Automatically update malicious code protection mechanisms as new releases are available in accordance with agency configuration management policy and procedures.
- Configure malicious code protection mechanisms to:
    - Perform periodic scans of the system and real-time scans of files from external sources at endpoint and/or network entry and exit points, as the files are downloaded, opened, or executed in accordance with agency policy.
    - Block malicious code, quarantine malicious code, or take agency-defined action, and send alerts to agency-defined personnel or roles in response to malicious code detection.
    - Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

System Monitoring (SI-4):

- Monitor the system to detect:
    - Attacks and indicators of potential attacks.
    - Unauthorized local, network, and remote connections.
- Identify unauthorized use of the system.
- Invoke internal monitoring capabilities or deploy monitoring devices:
    - Strategically within the system to collect agency-determined essential information.
    - At ad hoc locations within the system to track specific types of transactions of interest to the agency.
- Analyze detected events and anomalies.
- Adjust the level of system monitoring activity when there is a change in the risk to agency operations and assets, individuals, other organizations, or the Nation.
- Obtain legal opinion regarding system monitoring activities.
- Provide agency monitoring information to assigned personnel or roles as needed or by an agency-defined frequency.

System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis (SI-4(2)):

- Employ automated tools and mechanisms to support near real-time analysis of events.

System Monitoring | Inbound and Outbound Communications Traffic (SI-4(4)):

- Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic.
- Monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.

System Monitoring | System Generated Alerts (SI-4(5)):

- Alert agency-defined personnel or roles when the system generates indications of compromise or potential compromise occurs.

Security Alerts, Advisories, and Directives (SI-5):

- Receive system security alerts, advisories, and directives from agency-defined external organizations on an ongoing basis.
- Generate internal security alerts, advisories, and directives as deemed necessary.
- Disseminate security alerts, advisories, and directives to agency-defined personnel or roles.

- Implement security directives in accordance with established time frames. For Federal requirements, it may require the agency to notify the issuing organization of the degree of noncompliance.

Software, Firmware, and Information Integrity (SI-7):

- Employ integrity verification tools to detect unauthorized changes to software, firmware, and information.
- Take agency-defined actions when unauthorized changes to software, firmware, and information are detected.

Software, Firmware, and Information Integrity | Integrity Checks (SI-7(1)):

- Perform an integrity check of agency-defined software, firmware, and information at startup; at the identification of a new threat to which the information system is susceptible; the installation of new hardware, software, or firmware; or at an agency-defined frequency.

Software, Firmware, and Information Integrity | Integration of Detection and Response (SI-7(7)):

- Incorporate the detection of unauthorized changes into the agency incident response capability:
  - Unauthorized changes to baseline configuration setting.
  - Unauthorized elevation of system privileges.

Spam Protection (SI-8):

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

Spam Protection | Automatic Updates (SI-8(2)):

- Automatically update spam protection mechanisms on an agency-defined frequency.

Information Input Validation (SI-10):

- Check the validity of information inputs (e.g., character set, length, numerical range, acceptable values).

Error Handling (SI-11):

- Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.
- Reveal error messages only to designated agency officials.

Information Management and Retention (SI-12):

- Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements.

Information Management and Retention | Limit Personally Identifiable Information Elements (SI-12(1)):

- Limit personally identifiable information being processed in the information life cycle to agency-defined elements of PII.

Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research (SI-12(2)):

- Use agency-defined techniques to minimize the use of personally identifiable information for research, testing, or training.

Information Management and Retention | Information Disposal (SI-12(3)):

- Use agency-defined techniques to dispose of, destroy, or erase information following the retention period.

Memory Protection (SI-16):

- Implement controls to protect the system memory from unauthorized code execution. Controls employed to protect memory include data execution prevention (hardware-enforced or software-enforced) and address space layout randomization.

Personally Identifiable Information Quality Operations (SI-18):

- Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle on an agency-defined frequency.
- Correct or delete inaccurate or outdated personally identifiable information.

Personally Identifiable Information Quality Operations | Individual Requests (SI-18(4)):

- Correct or delete personally identifiable information upon request by individuals or their designated representatives.

De-Identification (SI-19):

- Remove agency-defined elements of personally identifiable information from datasets.
- Evaluate on an agency-defined frequency for effectiveness of de-identification.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies shall implement the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may also be subject to additional Federal, State, and/or Inter-agency regulatory requirements. It is each agency's responsibility to research and implement additional controls needed to meet regulatory compliance requirements and expectations outside of the State of Wisconsin baseline of controls.

Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions (SI-2(3)):

- Measure the time between flaw identification and flaw remediation.
- Establish agency-defined benchmarks for taking corrective actions.

System Monitoring | System-Wide Intrusion Detection System (SI-4(1)):

- Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.

System Monitoring | Analyze Communications Traffic Anomalies (SI-4(11)):

- Analyze outbound communications traffic at the external interfaces to the system and selected agency-defined interior points within the system to discover anomalies.

System Monitoring | Automated Agency-Generated Alerts (SI-4(12)):

- Alert appropriate agency personnel or roles using automated mechanisms when indications of inappropriate or unusual activities with security or privacy implications (i.e., agency-defined activities that trigger alerts) occur.

System Monitoring | Wireless Intrusion Detection (SI-4(14)):

- Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.

270 Personally Identifiable Information Processing and Transparency Standard

Purpose

The purpose of the Personally Identifiable Information Processing and Transparency Standard is to set forth requirements and expectations through the development of documentation related to and supporting standardized methods for how Personally Identifiable Information (PII) is accessed, processed, and shared within the State of Wisconsin computing environments.

This standard contains the minimum baseline controls that Executive Branch agencies shall implement; however, those agencies may also be required to implement controls outside of the scope of the controls listed in this document.

BASELINE CONTROLS

Policy and Procedures (PT-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
  - A personally identifiable information processing and transparency policy that:
    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
  - Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures.
- Review and update the current personally identifiable information processing and transparency:
  - Policy on an agency-defined frequency.
  - Procedures on an agency-defined frequency.

Authority to Process Personally Identifiable Information (PT-2):

- Determine and document the agency-defined authority that permits the processing of personally identifiable information.
- Restrict the access of personally identifiable information to only that which is authorized.

Personally Identifiable Information Processing Purposes (PT-3):

- Identify and document the purpose(s) for processing personally identifiable information.
- Describe the purpose(s) in the public privacy notices and policies of the agency.
- Restrict the processing of personally identifiable information to only that which is compatible with the identified purpose(s).
- Monitor changes in processing personally identifiable information and implement mechanisms to ensure that any changes are made in accordance with agency-defined requirements.

Consent (PT-4):

- Implement tools or mechanisms for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.

Privacy Notice (PT-5):

- Provide notice to individuals about the processing of personally identifiable information that:
  - Is available to individuals upon first interacting with the agency, and subsequently at an agency-defined frequency.
  - Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language.
  - Identifies the authority that authorizes the processing of personally identifiable information.
  - Identifies the purposes for which personally identifiable information is to be processed.
  - Includes agency-defined information.

Specific Categories of Personally Identifiable Information (PT-7):

- Apply agency-defined processing conditions for specific categories of personally identifiable information.

Specific Categories of PII | Social Security Numbers (PT-7(1)):

- When a system processes Social Security numbers:
  - Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier.
  - Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number.
  - Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

Specific Categories of PII | First Amendment Information (PT-7(2)):

- Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.

Additional Documentation

- NIST SP 800-53B https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf
- Wisconsin Statutes Chapter 19 General Duties of Public Officials, Subchapter IV PERSONAL INFORMATION PRACTICES https://docs.legis.wisconsin.gov/document/statutes/subch.%20IV%20of%20ch.%2019
- 5 USC 552a: Records maintained on individuals https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title5-section552a&num=0&edition=prelim
- Transparency: Wisconsin Statutes Chapter 19 General Duties of Public Officials, Subchapter II PUBLIC RECORDS AND PROPERTY https://docs.legis.wisconsin.gov/document/statutes/subch.%20II%20of%20ch.%2019
- Records of state offices and other public records.

https://docs.legis.wisconsin.gov/document/statutes/16.61

- Statewide General Records Schedules https://publicrecordsboard.wi.gov/Pages/GRS/Statewide.aspx

280 Supply Chain Risk Management Standard

Purpose

The purpose of the Supply Chain Risk Management Standard is to set forth requirements and expectations through the development of documentation related to, and supporting the supply chain and risk management framework to ensure that State of Wisconsin staff and business partners are well-informed of their responsibilities, and to maximize the State of Wisconsin information system environment uptime without delay or disruption.

Agencies have defined appropriations under Wisconsin Chapter 20 that determines what they are funded to do. This standard contains the minimum baseline controls that Executive Branch agencies shall implement; however, those agencies may also be required to implement controls outside of the scope of the controls listed in this document.

BASELINE CONTROLS

Policy and Procedures (SR-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
    - A supply chain risk management policy that:
        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
        - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
    - Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures.
- Review and update the current supply chain risk management:
    - Policy on an agency-defined frequency.
    - Procedures on an agency-defined frequency.

Supply Chain Risk Management Plan (SR-2):

- Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of agency-defined systems, system components, or system services.
- Review and update the supply chain risk management plan on an agency-defined frequency or as required, to address threat, organizational or environmental changes.
- Protect the supply chain risk management plan from unauthorized disclosure and modification.

Supply Chain Controls and Processes (SR-3):

- Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of agency-defined system or system component in coordination with supply chain personnel.
- Employ supply chain controls against supply chain risks to the system, system component, or system service to limit the harm or consequences from supply chain-related events.

- Document the selected and implemented supply chain processes and controls.

Acquisition Strategies, Tools, and Methods (SR-5):

- Employ acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks.

Supplier Assessments and Reviews (SR-6):

- Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide on an agency-defined frequency.

Notification Agreements (SR-8):

- Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises, the results of assessments or audits, or of agency-defined information.

Inspection of Systems or Components (SR-10):

- Inspect agency-defined systems or system components at random, at an agency-defined frequency, or upon agency-defined indications of need for inspection to detect tampering.

Component Authenticity (SR-11):

- Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system.
- Report counterfeit system components to agency-defined personnel or roles.

Anti-Counterfeit Training (SR-11(1)):

- Train agency-defined personnel or roles to detect counterfeit system components (including hardware, software, and firmware).

Configuration Control for Component Service and Repair (SR-11(2)):

- Maintain configuration control over agency-defined system components awaiting service or repair and serviced and repaired components awaiting return to service.

Component Disposal (SR-12):

- Dispose of agency-defined data, documentation, tools, or system components using agency-defined techniques and methods.

Additional Documentation

- Wisconsin Chapter 20 https://docs.legis.wisconsin.gov/document/statutes/20.505(1)(kL)

  "All moneys received for the provision of document sales services and services under ss. 16.971, 16.972, 16.973, 16.974 (3), and 16.997 (2) (d), other than moneys received and disbursed under par. (ip) and s. 20.225 (1) (kb), shall be credited to this appropriation account."
- Wis. Stat. § 16.971 (2) https://docs.legis.wisconsin.gov/statutes/statutes/16/vii/971
  The Department shall:

  (cm) Prescribe standards for data, application, and business process integration that shall be used by executive branch agencies, to the extent consistent with the statewide strategic plan formulated under par. (m), and that enable local governmental units to integrate their data,

application, and business processes into state systems whenever feasible.
(d) Develop review and approval procedures which encourage timely and cost-effective hardware, software, and professional services acquisitions, and review and approve the acquisition of such items and services under those procedures.

290 Removal of Prohibited Foreign Products Standard

Purpose

Pursuant to Governor Evers' Executive Order #184, the Removal of Prohibited Foreign Products Standard is intended to provide standardization on the removal of prohibited foreign products and technologies from State of Wisconsin IT Systems. This standard applies to all State of Wisconsin Executive Branch agencies, where statutorily authorized under subchapter VII of Chapter 16 but excluding the Board of Regents of the University of Wisconsin System. Executive Branch Agencies shall develop policies, procedures, or processes for their own State information and systems to protect State information, where applicable. Non-executive branch agencies are also strongly encouraged to adopt and implement this standard.

Standard

The Wisconsin Department of Administration (DOA) Division of Enterprise Technology (DET) is responsible for establishing, and has already established, security and safeguards for State information and information systems (Wis. Stat. §§ 16.971-16.975). DOA-DET is led by the State Chief Information Officer (State CIO) and State Chief Information Security Officer (State CISO) who continually monitors cybersecurity and implement all feasible technical means to ensure the security of all State information and information systems.

Using information gathered through state, federal, and industry-led intelligence, certain vendors, and products currently present an unacceptable level of cybersecurity risk to the State, including products and applications where the State has a reasonable belief that the manufacturer or vendor may participate in activities such as but not limited to:

- Collecting sensitive citizen, financial, proprietary, intellectual property, or other business data
- Enabling email compromise and acting as a vector for ransomware deployment
- Conducting cyber-espionage against government entities
- Conducting surveillance and tracking of individual users
- Using algorithmic modifications to conduct disinformation or misinformation campaigns.

Pursuant to Governor Evers' Executive Order #184 and Wis. Stat. §§ 16.971-16.975, DOA-DET shall continue to use information gathered through state, federal, and industry-led intelligence to investigate vulnerabilities presented by products from foreign vendors. If the State CISO determines that there are security vulnerabilities or deficiencies in any State information systems, the State CISO may determine and direct or take actions necessary to correct or remediate the vulnerabilities or deficiencies, which may include requiring the information system to be disconnected.

Products Subject to this Standard

Given that technology rapidly evolves and changes, it is not feasible to provide a complete list of prohibited products in this standard. In collaboration with the Governor, the Office of the Governor, and state, federal, and industry-led intelligence, DOA-DET shall continue to evaluate and identify applications and vendors. Due to the risk presented to state information or state information systems, the following list of applications/products are prohibited from being implemented on, or connected to any State network, or installed on any State-issued device, including but not limited to desktop computers, laptops, tablets, cellular phones, and other mobile devices.

The State CISO shall communicate any identified prohibited foreign products to the Wisconsin Information Sharing and Analysis Committee (WI ISAC) and Agency IT Directors, per DET's normal communications processes.

As of 7/28/2025, the following vendors and/or software are prohibited from being utilized:

- TikTok
- Huawei Technologies
- ZTE Corp
- Hytera Communications Corporation
- DeepSeek (all versions of DeepSeek)
- Hangzhou Hikvision Digital Technology Company
- Hangzhou DeepSeek Artificial Intelligence Co. LTD
- Dahua Technology Company
- Tencent Holdings, including but not limited to:
  - Tencent QQ
  - QQ Wallet
  - WeChat
- Alibaba products, including but not limited to:
  - AliPay
- Kaspersky Lab
- ByteDance

Required Actions

DOA-DET shall monitor adherence to this standard and assist impacted Executive Branch agencies to ensure they are able to comply with this standard. DOA/DET, the State CIO, and State CISO shall provide support including, but not limited to:

- Developing and implementing a plan to remove any prohibited hardware products from State networks.
- Removing any prohibited software products on State networks.
- Implementing measures to prevent the installation of prohibited hardware and software products on State-owned, State-leased, or State-managed technology assets.
- Implementing network-based restrictions to prevent the use of, or access to, prohibited services.
- Incorporating the risks associated with these technologies into security awareness training.

Compliance References

240_System_and_Services_Acquisition_Standard_Executive_Branch.pdf (wi.gov)
280_Supply_Chain_Risk_Management.pdf (wi.gov)
Official Website for Wisconsin Governor Tony Evers Executive Orders
Wisconsin Legislature: 16.754
https://www.gsa.gov/

500 Program Management Standard

Purpose

The purpose of the Program Management standard is to facilitate the attainment of the Program Management Policy and associated Information Technology (IT) Security objectives.

This standard is divided into two sections of controls. **Section One** contains the minimum baseline controls that Executive Branch agencies shall implement. Section Two contains some of the common, regulatory controls agencies may be required to implement in addition to the baseline controls. Section Two is not all-inclusive. Each agency is responsible for identifying what other controls their agency may be required to implement beyond the scope of this standard.

SECTION ONE: BASELINE CONTROLS

Information Security Program Plan (PM-1):

- Develop and disseminate an agency-wide information security program plan that:
  - Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.
  - Includes the identification and assignment of roles, responsibilities, management commitment, coordination among agency entities, and compliance.
  - Reflects the coordination among agency entities responsible for information security.
  - Is approved by a senior official with responsibility and accountability for the risk being incurred to agency operations (including mission, functions, image, and reputation), agency assets, individuals, other agencies, and the State.
- Review and update the agency-wide information security program plan on an agency-defined frequency and following agency-defined events.
- Protect the information security program plan from unauthorized disclosure and modification.

Plan of Action and Milestones Process (PM-4):

- Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated agency systems:
  - Are developed and maintained.
  - Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to agency operations and assets, individuals, other organizations, and the State.
  - Are reported in accordance with established reporting requirements.
- Review plans of action and milestones for consistency with the agency risk management strategy and organization-wide priorities for risk response actions.

System Inventory (PM-5):

- Develop and update on an agency-defined frequency an inventory of agency systems.

System Inventory | Inventory of Personally Identifiable Information (PM-5(1)):

- Establish, maintain, and update on an agency-defined frequency an inventory of all systems, applications, and projects that process personally identifiable information.

Enterprise Architecture (PM-7):

- Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to agency operations and assets, individuals, other organizations, and the State.

Risk Management Strategy (PM-9):

- Develop a comprehensive strategy to manage:
    - Security risk to agency operations and assets, individuals, other organizations, and the State associated with the operation and use of agency systems.
    - Privacy risk to individuals resulting from the authorized processing of personally identifiable information.
- Implement the risk management strategy consistently across the agency.
- Review and update the risk management strategy every three (3) years or as required, to address agency changes.

Authorization Process (PM-10):

- Manage the security and privacy state of agency systems and the environments in which those systems operate through authorization processes.
- Designate individuals to fulfill specific roles and responsibilities within the agency risk management process.
- Integrate the authorization process into an agency-wide risk management program.

Mission and Business Process Definition (PM-11):

- Define agency mission and business processes with consideration for information security and privacy and the resulting risk to agency operations, agency assets, individuals, other organizations, and the State.
- Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes.
- Review and revise the mission and business process on an agency-defined frequency.

Testing, Training, and Monitoring (PM-14):

- Implement a process for ensuring that agency plans for conducting security and privacy testing, training, and monitoring activities associated with agency systems:
    - Are developed and maintained.
    - Continue to be executed.
- Review testing, training, and monitoring plans for consistency with the agency risk management strategy and agency-wide priorities for risk response actions.

Privacy Program Plan (PM-18):

- Develop and disseminate an agency-wide privacy program plan that provides an overview of the agency's privacy program, and:
    - Includes a description of the structure of the privacy program and the resources dedicated to the privacy program.
    - Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements.
    - Includes the role of the senior agency official for privacy and the identification and

assignment of roles of other privacy officials and staff and their responsibilities.
  - Describes management commitment, compliance, and the strategic goals and objectives of the privacy program.
  - Reflects coordination among agency entities responsible for the different aspects of privacy.
  - Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to agency operations (including mission, functions, image, and reputation), agency assets, individuals, other organizations, and the State.
- Update the plan on an agency-defined frequency to address changes in state and federal privacy laws and policy and agency changes and problems identified during plan implementation or privacy control assessments.

Minimization of Personally Identifiable Information Used in Testing, Training, and Research (PM-25):

- Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research.
- Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes.
- Authorize the use of personally identifiable information when such information is required for internal testing, training, and research.
- Review and update policies and procedures on an annual basis.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies shall implement the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may also be subject to additional Federal, State, and/or Inter-agency regulatory requirements. It is each agency's responsibility to research and implement additional controls needed to meet regulatory compliance requirements and expectations outside of the State of Wisconsin baseline of controls.

Information Security and Privacy Resources (PM-3):

- Include the resources needed to implement the information security and privacy programs in capital management planning and investment requests and document all exceptions to the requirement.
- Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, and standards.
- Make available for expenditure, the planned information security and privacy resources.

Insider Threat Program (PM-12):

- Implement an insider threat program that includes a cross-discipline insider incident handling team.

APPENDICES

Appendix A – Definitions

Executive Branch Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies. Agency or State Agency may be used interchangeably with Executive Branch Agency.

State information - Any information/data that is created, accessed, used, stored, or transmitted by an Executive Branch Agency.

State information systems and system environments - All equipment or services used to input, store, process, transmit, and output information, including, but not limited to network devices, servers, databases, printers, internet, email, physical, virtual, cloud, and applications accessible to and/or managed by the agency.

Identified Account Types - Include: Individual, privileged (administrative and default privileged), shared, service, emergency, and temporary accounts (temporary and guest wireless account) (AC-2).

Control Baseline – A control baseline is a collection of controls assembled to address the protection needs of a group, organization, or community of interest. It provides a generalized set of controls that represent a starting point for the subsequent tailoring activities that are applied to the baseline to produce a targeted or customized security and privacy solution for the entity that the baseline is intended to serve.

Relying Party - An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.

Appendix B – Exception Process

Exceptions to any Executive Branch Agency's Security Policies or Standards shall follow the Executive Branch Risk Exception Procedure.

Appendix C – Matrix - Controls Selected for 2025 Standards

100 Access Control Standard

The following table includes the baseline controls in the Access Control Standard

CONTROL	CONTROL NAME	PRIVACY	SECURITY CONTROL			IRS	MARS-E	CJIS 6.0	HIPAA Security	FERPA	ISO	PCI-DSS
NUMBER	CONTROL ENHANCEMENT NAME	CONTROL	LOW	MOD	HIGH	Publication	2.2		Rule 45 C.F.R		270001	v4.0.1
AC-1	Policy and Procedures	x	x	x	x	x	x	x			x	x
AC-2	Account Management		x	x	x	x	x	x	x		x	x
AC-2(1)	AUTOMATED SYSTEM ACCOUNT MANAGEMENT			x	x	x	x	x				
AC-2(2)	AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT			x	x	x	x	x				
AC-2(3)	DISABLE ACCOUNTS			x	x	x	x	x				x
AC-2(4)	AUTOMATED AUDIT ACTIONS			x	x	x	x	x				
AC-2(5)	INACTIVITY LOGOUT			x	x		x	x				x
AC-2(13)	DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS			x	x	x		x				x
AC-3	Access Enforcement		x	x	x	x	x	x	x	x	x	x
AC-3(14)	INDIVIDUAL ACCESS	x						x				
AC-4	Information Flow Enforcement			x	x	x	x	x	x		x	x
AC-5	Separation of Duties			x	x	x	x	x	x		x	x
AC-6	Least Privilege			x	x	x	x	x	x	x	x	x
AC-6(1)	AUTHORIZE ACCESS TO SECURITY FUNCTIONS			x	x	x	x	x				
AC-6(2)	NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS			x	x	x	x	x				
AC-6(5)	PRIVILEGED ACCOUNTS			x	x		x	x				x
AC-6(7)	REVIEW OF USER PRIVILEGES			x	x	x		x				x
AC-6(9)	LOG USE OF PRIVILEGED FUNCTIONS			x	x	x	x	x				x
AC-6(10)	PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS			x	x	x	x	x				
AC-7	Unsuccessful Logon Attempts		x	x	x	x	x	x			x	x
AC-8	System Use Notification		x	x	x	x	x	x			x	
AC-11	Device Lock			x	x	x	x	x			x	x
AC-11(1)	PATTERN-HIDING DISPLAYS			x	x	x	x	x				
AC-12	Session Termination			x	x	x	x	x			-	x
AC-14	Permitted Actions without Identification or Authentication		x	x	x	x	x	x			-	
AC-20	Use of External Systems		x	x	x	x	x	x	x		x	
AC-20(1)	LIMITS ON AUTHORIZED USE			x	x		x	x				x
AC-20(2)	PORTABLE STORAGE DEVICES — RESTRICTED USE			x	x	x	x	x				
AC-21	Information Sharing			x	x	x	x	x	x		-	
AC-22	Publicly Accessible Content		x	x	x	x	x	x			-	x

The following table includes additional regulatory controls for agencies with regulatory requirements

CONTROL	CONTROL NAME	PRIVACY	SECURITY CONTROL			IRS	MARS-E	CJIS 6.0	HIPAA Security	FERPA	ISO	PCI-DSS
NUMBER	CONTROL ENHANCEMENT NAME	CONTROL	LOW	MOD	HIGH	Publication	2.2		Rule 45 C.F.R		270001	v4.0.1
AC-2(7)	PRIVILEGED USER ACCOUNTS					x	x					x
AC-2(9)	RESTRICTIONS ON USE OF SHARED AND GROUP ACCOUNTS					x	x					x
AC-2(12)	ACCOUNT MONITORING FOR ATYPICAL USAGE				x	x	x					x
AC-3(9)	CONTROLLED RELEASE					x	x					
AC-10	Concurrent Session Control				x		x				-	
AC-12(1)	USER-INITIATED LOGOUTS					x						
AC-20(3)	NON-ORGANIZATIONALLY OWNED SYSTEMS — RESTRICTED USE					x	x					
AC-23	Data Mining Protection					x					-	x

The following controls were not selected to be included in the standard

CONTROL	CONTROL NAME	PRIVACY	SECURITY CONTROL			IRS	MARS-E	CJIS 6.0	HIPAA Security	FERPA	ISO	PCI-DSS
NUMBER	CONTROL ENHANCEMENT NAME	CONTROL	LOW	MOD	HIGH	Publication	2.2		Rule 45 C.F.R		270001	v4.0.1
AC-2(6)	DYNAMIC PRIVILEGE MANAGEMENT											
AC-2(8)	DYNAMIC ACCOUNT MANAGEMENT											
AC-2(11)	USAGE CONDITIONS				x							
AC-3(2)	DUAL AUTHORIZATION											
AC-3(3)	MANDATORY ACCESS CONTROL											
AC-3(4)	DISCRETIONARY ACCESS CONTROL											

AC-3(5)	SECURITY-RELEVANT INFORMATION											
AC-3(7)	ROLE-BASED ACCESS CONTROL											
AC-3(8)	REVOCATION OF ACCESS AUTHORIZATIONS											x
AC-3(10)	AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS											
AC-3(11)	RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES					x						
AC-3(12)	ASSERT AND ENFORCE APPLICATION ACCESS											
AC-3(13)	ATTRIBUTE-BASED ACCESS CONTROL											
AC-3(15)	DISCRETIONARY AND MANDATORY ACCESS CONTROL											
AC-4(1)	OBJECT SECURITY AND PRIVACY ATTRIBUTES											
AC-4(2)	PROCESSING DOMAINS											
AC-4(3)	DYNAMIC INFORMATION FLOW CONTROL											
AC-4(4)	FLOW CONTROL OF ENCRYPTED INFORMATION				x							
AC-4(5)	EMBEDDED DATA TYPES											
AC-4(6)	METADATA											
AC-4(7)	ONE-WAY FLOW MECHANISMS											
AC-4(8)	SECURITY AND PRIVACY POLICY FILTERS											x
AC-4(9)	HUMAN REVIEWS											x
AC-4(10)	ENABLE AND DISABLE SECURITY OR PRIVACY POLICY FILTERS											
AC-4(11)	CONFIGURATION OF SECURITY OR PRIVACY POLICY FILTERS											
AC-4(12)	DATA TYPE IDENTIFIERS											
AC-4(13)	DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS											
AC-4(14)	SECURITY OR PRIVACY POLICY FILTER CONSTRAINTS											
AC-4(15)	DETECTION OF UNSANCTIONED INFORMATION											
AC-4(17)	DOMAIN AUTHENTICATION											
AC-4(19)	VALIDATION OF METADATA											
AC-4(20)	APPROVED SOLUTIONS											
AC-4(21)	PHYSICAL OR LOGICAL SEPARATION OF INFORMATION FLOWS						x					x
AC-4(22)	ACCESS ONLY											
AC-4(23)	MODIFY NON-RELEASABLE INFORMATION											
AC-4(24)	INTERNAL NORMALIZED FORMAT											
AC-4(25)	DATA SANITIZATION											x
AC-4(26)	AUDIT FILTERING ACTIONS											
AC-4(27)	REDUNDANT/INDEPENDENT FILTERING MECHANISMS											
AC-4(28)	LINEAR FILTER PIPELINES											
AC-4(29)	FILTER ORCHESTRATION ENGINES											
AC-4(30)	FILTER MECHANISMS USING MULTIPLE PROCESSES											
AC-4(31)	FAILED CONTENT TRANSFER PREVENTION											
AC-4(32)	PROCESS REQUIREMENTS FOR INFORMATION TRANSFER											
AC-6(3)	NETWORK ACCESS TO PRIVILEGED COMMANDS				x							
AC-6(4)	SEPARATE PROCESSING DOMAINS											
AC-6(6)	PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS					x						
AC-6(8)	PRIVILEGE LEVELS FOR CODE EXECUTION					x						
AC-7(2)	PURGE OR WIPE MOBILE DEVICE					x						
AC-7(3)	BIOMETRIC ATTEMPT LIMITING											
AC-7(4)	USE OF ALTERNATE AUTHENTICATION FACTOR											
AC-9	Previous Logon Notification										x	
AC-9(1)	UNSUCCESSFUL LOGONS											
AC-9(2)	SUCCESSFUL AND UNSUCCESSFUL LOGONS											
AC-9(3)	NOTIFICATION OF ACCOUNT CHANGES											
AC-9(4)	ADDITIONAL LOGON INFORMATION											
AC-12(2)	TERMINATION MESSAGE											
AC-12(3)	TIMEOUT WARNING MESSAGE											
AC-16	Security and Privacy Attributes								x		-	

AC-16(1)	DYNAMIC ATTRIBUTE ASSOCIATION											
AC-16(2)	ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS											
AC-16(3)	MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY SYSTEM											
AC-16(4)	ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS											
AC-16(5)	ATTRIBUTE DISPLAYS ON OBJECTS TO BE OUTPUT											
AC-16(6)	MAINTENANCE OF ATTRIBUTE ASSOCIATION											
AC-16(7)	CONSISTENT ATTRIBUTE INTERPRETATION											
AC-16(8)	ASSOCIATION TECHNIQUES AND TECHNOLOGIES											
AC-16(9)	ATTRIBUTE REASSIGNMENT – REGRADING MECHANISMS											
AC-16(10)	ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS											
AC-20(4)	NETWORK ACCESSIBLE STORAGE DEVICES — PROHIBITED USE											
AC-20(5)	PORTABLE STORAGE DEVICES — PROHIBITED USE					x						
AC-21(1)	AUTOMATED DECISION SUPPORT											
AC-21(2)	INFORMATION SEARCH AND RETRIEVAL											
AC-24	Access Control Decisions										x	
AC-24(1)	TRANSMIT ACCESS AUTHORIZATION INFORMATION											
AC-24(2)	NO USER OR PROCESS IDENTITY											
AC-25	Reference Monitor										-	

101 Access Control for Remote Access Standard

The following table includes the baseline controls in the Access Control for Remote Access Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
AC-17	Remote Access (See 101 Access Control for Remote Standard)		x	x	x	x	x	x	x		x	x
AC-17(1)	MONITORING AND CONTROL			x	x	x	x	x				
AC-17(2)	PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION			x	x	x	x	x				
AC-17(3)	MANAGED ACCESS CONTROL POINTS			x	x	x	x	x				
AC-17(4)	PRIVILEGED COMMANDS AND ACCESS			x	x	x	x	x				

The following table includes additional regulatory controls for agencies with regulatory requirements

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
AC-17(9)	DISCONNECT OR DISABLE ACCESS					x	x					

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL	SECURITY CONTROL			IRS Publication	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
AC-17(6)	PROTECTION OF MECHANISM INFORMATION											x
AC-17(10)	AUTHENTICATE REMOTE COMMANDS											

102 Access Control for Wireless Access Standard

The following table includes the baseline controls for the Access Control for Wireless Access Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
AC-18	Wireless Access (See 102 Access Control for Wireless Access Standard)		x	x	x	x	x	x	x		x	x
AC-18(1)	AUTHENTICATION AND ENCRYPTION			x	x	x	x	x				x
AC-18(3)	DISABLE WIRELESS NETWORKING			x	x	x		x				

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
AC-18(4)	RESTRICT CONFIGURATIONS BY USERS				x							
AC-18(5)	ANTENNAS AND TRANSMISSION POWER LEVELS				x							

103 Access Control for Mobile Device Security Standard

The following table includes the baseline controls in the Access Control for Mobile Device Security Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
AC-19	Access Control for Mobile Devices (See 103 Access Control for Mobile Device Security Standard)		x	x	x	x	x	x	x	x	x	
AC-19(5)	FULL DEVICE OR CONTAINER-BASED ENCRYPTION			x	x	x	x	x				

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
AC-19(4)	RESTRICTIONS FOR CLASSIFIED INFORMATION											

110 Security Awareness and Training Standard

The following table includes the baseline controls for the Security Awareness and Training Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
AT-1	Policy and Procedures	x	x	x	x	x	x	x		x	x	x
AT-2	Literacy Training and Awareness	x	x	x	x	x	x	x	x	x	x	x
AT-2(2)	INSIDER THREAT		x	x	x	x	x	x				
AT-2(3)	SOCIAL ENGINEERING AND MINING			x	x	x		x				x
AT-3	Role-Based Training	x	x	x	x	x	x	x	x		x	x
AT-3(5)	PROCESSING PERSONALLY IDENTIFIABLE INFORMATION	x						x				x
AT-4	Training Records	x	x	x	x	x	x	x			-	x

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
AT-2(1)	PRACTICAL EXERCISES					x						
AT-2(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR					x						x
AT-2(5)	ADVANCED PERSISTENT THREAT											x
AT-2(6)	CYBER THREAT ENVIRONMENT											x
AT-3(1)	ENVIRONMENTAL CONTROLS											
AT-3(2)	PHYSICAL SECURITY CONTROLS											x
AT-3(3)	PRACTICAL EXERCISES											
AT-6	Training Feedback					x					-	

120 Audit and Accountability Standard

The following table includes the baseline controls for the Audit and Accountability Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
AU-1	Policy and Procedures	x	x	x	x	x	x	x	x		x	x
AU-2	Event Logging	x	x	x	x	x	x	x	x		-	x
AU-3	Content of Audit Records		x	x	x	x	x	x	x		x	x
AU-3(1)	ADDITIONAL AUDIT INFORMATION			x	x	x	x	x				
AU-3(3)	LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	x				x		x				
AU-4	Audit Log Storage Capacity		x	x	x	x	x	x	x		x	
AU-5	Response to Audit Logging Process Failures		x	x	x	x	x	x	x		-	
AU-6	Audit Record Review, Analysis, and Reporting		x	x	x	x	x	x	x		x	x
AU-6(1)	AUTOMATED PROCESS INTEGRATION			x	x	x	x	x				
AU-6(3)	CORRELATE AUDIT RECORD REPOSITORIES			x	x	x	x	x				x

AU-7	Audit Record Reduction and Report Generation			x	x	x	x	x	x		-	
AU-7(1)	AUTOMATIC PROCESSING			x	x	x	x	x				
AU-8	Time Stamps		x	x	x	x	x	x	x		x	x
AU-9	Protection of Audit Information		x	x	x	x	x	x	x		x	x
AU-9(4)	ACCESS BY SUBSET OF PRIVILEGED USERS			x	x	x	x	x				x
AU-11	Audit Record Retention	x	x	x	x	x	x	x	x		x	x
AU-12	Audit Record Generation		x	x	x	x	x	x	x		x	

The following table includes additional regulatory controls for agencies with regulatory requirements

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
AU-5(1)	STORAGE CAPACITY WARNING				x	x						
AU-9(2)	STORE ON SEPARATE PHYSICAL SYSTEMS OR COMPONENTS				x		x					x

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
AU-4(1)	TRANSFER TO ALTERNATE STORAGE											x
AU-5(2)	REAL-TIME ALERTS				x							
AU-5(3)	CONFIGURABLE TRAFFIC VOLUME THRESHOLDS											
AU-5(4)	SHUTDOWN ON FAILURE											
AU-5(5)	ALTERNATE AUDIT LOGGING CAPABILITY											
AU-6(4)	CENTRAL REVIEW AND ANALYSIS											x
AU-6(5)	INTEGRATED ANALYSIS OF AUDIT RECORDS				x							
AU-6(6)	CORRELATION WITH PHYSICAL MONITORING				x							
AU-6(7)	PERMITTED ACTIONS					x						
AU-6(8)	FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS											x
AU-6(9)	CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES					x						x
AU-9(1)	HARDWARE WRITE-ONCE MEDIA											
AU-9(3)	CRYPTOGRAPHIC PROTECTION				x							
AU-9(5)	DUAL AUTHORIZATION											
AU-9(6)	READ-ONLY ACCESS											
AU-9(7)	STORE ON COMPONENT WITH DIFFERENT OPERATING SYSTEM											
AU-10	Non-repudiation				x						-	
AU-10(1)	ASSOCIATION OF IDENTITIES											
AU-10(2)	VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY											
AU-10(3)	CHAIN OF CUSTODY											
AU-10(4)	VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY											
AU-11(1)	LONG-TERM RETRIEVAL CAPABILITY											
AU-12(1)	SYSTEM-WIDE AND TIME-CORRELATED AUDIT TRAIL				x	x						x
AU-12(2)	STANDARDIZED FORMATS											
AU-12(3)	CHANGES BY AUTHORIZED INDIVIDUALS				x							
AU-12(4)	QUERY PARAMETER AUDITS OF PERSONALLY IDENTIFIABLE INFORMATION											
AU-13	Monitoring for Information Disclosure								x		-	
AU-13(1)	USE OF AUTOMATED TOOLS											
AU-13(2)	REVIEW OF MONITORED SITES											
AU-13(3)	UNAUTHORIZED REPLICATION OF INFORMATION											
AU-14	Session Audit										x	
AU-14(1)	SYSTEM START-UP											
AU-14(3)	REMOTE VIEWING AND LISTENING											
AU-16	Cross-Organizational Audit Logging					x					-	
AU-16(1)	IDENTITY PRESERVATION					x						
AU-16(2)	SHARING OF AUDIT INFORMATION					x						
AU-16(3)	DISASSOCIABILITY											

130 Security Assessment and Authorization Standard

The following table includes the baseline controls for the Security Assessment and Authorization Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
CA-1	Policy and Procedures	x	x	x	x	x	x	x			x	x
CA-2	Control Assessments	x	x	x	x	x	x	x	x	x	x	x
CA-2(1)	INDEPENDENT ASSESSORS			x	x	x	x	x				
CA-3	Information Exchange		x	x	x	x	x	x	x		x	
CA-5	Plan of Action and Milestones	x	x	x	x	x	x	x			x	
CA-6	Authorization	x	x	x	x	x	x	x	x		x	
CA-7	Continuous Monitoring	x	x	x	x	x	x	x	x		x	x
CA-7(1)	INDEPENDENT ASSESSMENT			x	x	x	x	x				x
CA-7(4)	RISK MONITORING	x	x	x	x	x		x				
CA-9	Internal System Connections		x	x	x	x	x	x	x		-	

The following table includes additional regulatory controls for agencies with regulatory requirements

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
CA-8	Penetration Testing				x	x	x		x		-	x

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
CA-2(2)	SPECIALIZED ASSESSMENTS				x							
CA-2(3)	LEVERAGING RESULTS FROM EXTERNAL ORGANIZATIONS											
CA-3(6)	TRANSFER AUTHORIZATIONS				x							
CA-3(7)	TRANSITIVE INFORMATION EXCHANGES											
CA-5(1)	AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY											
CA-6(1)	JOINT AUTHORIZATION — INTRA-ORGANIZATION											
CA-6(2)	JOINT AUTHORIZATION — INTER-ORGANIZATION											
CA-7(3)	TREND ANALYSES											
CA-7(5)	CONSISTENCY ANALYSIS											
CA-7(6)	AUTOMATION SUPPORT FOR MONITORING											
CA-8(1)	INDEPENDENT PENETRATION TESTING AGENT OR TEAM				x		x					x
CA-8(2)	RED TEAM EXERCISES											
CA-8(3)	FACILITY PENETRATION TESTING											
CA-9(1)	COMPLIANCE CHECKS					x						

140 Configuration Management Standard

The following table includes the baseline controls in the Configuration Management Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
CM-1	Policy and Procedures	x	x	x	x	x	x	x			x	x
CM-2	Baseline Configuration		x	x	x	x	x	x	x	x	-	x
CM-2(2)	AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY			x	x	x	x	x				
CM-2(3)	RETENTION OF PREVIOUS CONFIGURATIONS			x	x	x	x	x				
CM-2(7)	CONFIGURE SYSTEMS AND COMPONENTS FOR HIGH-RISK AREAS			x	x	x	x	x				x
CM-3	Configuration Change Control			x	x	x	x	x	x	x	x	x
CM-3(2)	TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES			x	x	x	x	x				x
CM-3(4)	SECURITY AND PRIVACY REPRESENTATIVES			x	x	x		x				
CM-4	Impact Analyses	x	x	x	x	x	x	x	x		x	x
CM-4(2)	VERIFICATION OF CONTROLS			x	x	x	x	x				
CM-5	Access Restrictions for Change		x	x	x	x	x	x	x		x	x
CM-6	Configuration Settings		x	x	x	x	x	x	x	x	-	x
CM-7	Least Functionality		x	x	x	x	x	x	x		x	x
CM-7(1)	PERIODIC REVIEW			x	x	x	x	x				x
CM-7(2)	PREVENT PROGRAM EXECUTION			x	x		x	x				
CM-7(5)	AUTHORIZED SOFTWARE — ALLOW-BY-EXCEPTION			x	x	x	x	x				
CM-8	System Component Inventory		x	x	x	x	x	x	x	x	x	x
CM-8(1)	UPDATES DURING INSTALLATION AND REMOVAL			x	x	x	x	x				
CM-8(3)	AUTOMATED UNAUTHORIZED COMPONENT DETECTION			x	x	x	x	x				
CM-9	Configuration Management Plan			x	x	x	x	x	x		x	x
CM-10	Software Usage Restrictions		x	x	x	x	x	x	x		x	
CM-11	User-Installed Software		x	x	x	x	x	x	x		x	
CM-12	Information Location			x	x	x		x			-	
CM-12(1)	AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION			x	x	x		x				

The following table includes additional regulatory controls for agencies with regulatory requirements

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
CM-4(1)	SEPARATE TEST ENVIRONMENTS				x		x					x
CM-5(1)	AUTOMATED ACCESS ENFORCEMENT AND AUDIT RECORDS				x		x					
CM-5(5)	PRIVILEGE LIMITATION FOR PRODUCTION AND OPERATION					x	x					

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
CM-2(6)	DEVELOPMENT AND TEST ENVIRONMENTS											x
CM-3(1)	AUTOMATED DOCUMENTATION, NOTIFICATION, AND PROHIBITION OF CHANGES				x							x
CM-3(3)	AUTOMATED CHANGE IMPLEMENTATION											
CM-3(5)	AUTOMATED SECURITY RESPONSE											x
CM-3(6)	CRYPTOGRAPHY MANAGEMENT				x							
CM-3(7)	REVIEW SYSTEM CHANGES											x
CM-3(8)	PREVENT OR RESTRICT CONFIGURATION CHANGES											
CM-5(4)	DUAL AUTHORIZATION											
CM-5(6)	LIMIT LIBRARY PRIVILEGES											
CM-6(1)	AUTOMATED MANAGEMENT, APPLICATION, AND VERIFICATION				x		x					
CM-6(2)	RESPOND TO UNAUTHORIZED CHANGES				x							x
CM-7(3)	REGISTRATION COMPLIANCE											
CM-7(4)	UNAUTHORIZED SOFTWARE — DENY-BY-EXCEPTION											
CM-7(6)	CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES											x
CM-7(7)	CODE EXECUTION IN PROTECTED ENVIRONMENTS											x
CM-7(8)	BINARY OR MACHINE EXECUTABLE CODE											
CM-7(9)	PROHIBITING THE USE OF UNAUTHORIZED HARDWARE					x						x
CM-8(2)	AUTOMATED MAINTENANCE				x							
CM-8(4)	ACCOUNTABILITY INFORMATION				x							
CM-8(6)	ASSESSED CONFIGURATIONS AND APPROVED DEVIATIONS											
CM-8(7)	CENTRALIZED REPOSITORY											
CM-8(8)	AUTOMATED LOCATION TRACKING											
CM-8(9)	ASSIGNMENT OF COMPONENTS TO SYSTEMS											
CM-9(1)	ASSIGNMENT OF RESPONSIBILITY											x
CM-10(1)	OPEN-SOURCE SOFTWARE						x					
CM-11(2)	SOFTWARE INSTALLATION WITH PRIVILEGED STATUS											
CM-11(3)	AUTOMATED ENFORCEMENT AND MONITORING											
CM-13	Data Action Mapping					x					-	
CM-14	Signed Components					x					-	

150 Contingency Planning Standard

The following table includes the baseline controls for the Contingency Planning Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
CP-1	Policy and Procedures		x	x	x	x	x	x			x	x
CP-2	Contingency Plan		x	x	x	x	x	x	x		x	
CP-2(1)	COORDINATE WITH RELATED PLANS			x	x	x	x	x				
CP-2(3)	RESUME MISSION AND BUSINESS FUNCTIONS			x	x	x	x	x				
CP-2(8)	IDENTIFY CRITICAL ASSETS			x	x	x	x	x				
CP-3	Contingency Training		x	x	x	x	x	x	x		x	
CP-4	Contingency Plan Testing		x	x	x	x	x	x	x		x	
CP-4(1)	COORDINATE WITH RELATED PLANS			x	x	x	x	x				
CP-6	Alternate Storage Site			x	x		x	x	x		x	
CP-6(1)	SEPARATION FROM PRIMARY SITE			x	x		x	x				
CP-6(3)	ACCESSIBILITY			x	x		x	x				
CP-7	Alternate Processing Site			x	x		x	x			x	
CP-7(1)	SEPARATION FROM PRIMARY SITE			x	x		x	x				
CP-7(2)	ACCESSIBILITY			x	x		x	x				
CP-7(3)	PRIORITY OF SERVICE			x	x		x	x				
CP-8	Telecommunications Services			x	x		x	x	x		x	
CP-8(1)	PRIORITY OF SERVICE PROVISIONS			x	x		x	x				
CP-8(2)	SINGLE POINTS OF FAILURE			x	x		x	x				
CP-9	System Backup		x	x	x	x	x	x	x		x	x
CP-9(1)	TESTING FOR RELIABILITY AND INTEGRITY			x	x		x	x				
CP-9(8)	CRYPTOGRAPHIC PROTECTION			x	x	x		x				
CP-10	System Recovery and Reconstitution		x	x	x	x	x	x	x		x	
CP-10(2)	TRANSACTION RECOVERY			x	x	x	x	x				

The following table includes additional regulatory controls for agencies with regulatory requirements

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
CP-2(2)	CAPACITY PLANNING				x		x					

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
CP-2(5)	CONTINUE MISSION AND BUSINESS FUNCTIONS				x							
CP-2(6)	ALTERNATE PROCESSING AND STORAGE SITES											
CP-2(7)	COORDINATE WITH EXTERNAL SERVICE PROVIDERS											
CP-3(1)	SIMULATED EVENTS				x							
CP-3(2)	MECHANISMS USED IN TRAINING ENVIRONMENTS											
CP-4(2)	ALTERNATE PROCESSING SITE				x							
CP-4(3)	AUTOMATED TESTING											
CP-4(4)	FULL RECOVERY AND RECONSTITUTION											
CP-4(5)	SELF-CHALLENGE											
CP-6(2)	RECOVERY TIME AND RECOVERY POINT OBJECTIVES				x							
CP-7(4)	PREPARATION FOR USE				x							
CP-7(6)	INABILITY TO RETURN TO PRIMARY SITE											
CP-8(3)	SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS				x							
CP-8(4)	PROVIDER CONTINGENCY PLAN				x							
CP-8(5)	ALTERNATE TELECOMMUNICATION SERVICE TESTING											
CP-9(2)	TEST RESTORATION USING SAMPLING				x							
CP-9(3)	SEPARATE STORAGE FOR CRITICAL INFORMATION				x		x					x
CP-9(5)	TRANSFER TO ALTERNATE STORAGE SITE				x							
CP-9(6)	REDUNDANT SECONDARY SYSTEM											
CP-9(7)	DUAL AUTHORIZATION FOR DELETION OR DESTRUCTION											
CP-10(4)	RESTORE WITHIN TIME PERIOD				x							
CP-10(6)	COMPONENT PROTECTION											
CP-11	Alternate Communications Protocols								x		x	
CP-12	Safe Mode										-	
CP-13	Alternative Security Mechanisms										x	

160 Identification and Authentication Standard

The following table includes the baseline controls for the Identification and Authentication Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
IA-1	Policy and Procedures		x	x	x	x	x	x	x		x	x
IA-2	Identification and Authentication (Organizational Users)		x	x	x	x	x	x	x	x	x	x
IA-2(1)	MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS		x	x	x	x	x	x				x
IA-2(2)	MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS		x	x	x	x	x	x				x
IA-2(8)	ACCESS TO ACCOUNTS — REPLAY RESISTANT		x	x	x	x	x	x				x
IA-2(12)	ACCEPTANCE OF PIV CREDENTIALS		x	x	x			x				
IA-3	Device Identification and Authentication			x	x	x	x	x			-	
IA-4	Identifier Management		x	x	x	x	x	x	x		x	x
IA-4(4)	IDENTIFY USER STATUS			x	x	x	x	x				x
IA-5	Authenticator Management		x	x	x	x	x	x	x		x	x
IA-5(1)	PASSWORD-BASED AUTHENTICATION		x	x	x	x	x	x				x
IA-5(2)	PUBLIC KEY-BASED AUTHENTICATION			x	x	x	x	x				x
IA-5(6)	PROTECTION OF AUTHENTICATORS			x	x	x	x	x				x
IA-6	Authentication Feedback		x	x	x	x	x	x	x		x	
IA-7	Cryptographic Module Authentication		x	x	x	x	x	x	x		x	x
IA-8	Identification and Authentication (Non-Organizational Users)		x	x	x	x	x	x	x		x	x
IA-8(1)	ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES		x	x	x			x				
IA-8(2)	ACCEPTANCE OF EXTERNAL AUTHENTICATORS		x	x	x	x	x	x				x
IA-8(4)	USE OF DEFINED PROFILES		x	x	x	x	x	x				
IA-11	Re-authentication		x	x	x	x		x			-	x
IA-12	Identity Proofing			x	x	x		x			-	x
IA-12(1)	SUPERVISOR AUTHORIZATION			x	x	x						
IA-12(2)	IDENTITY EVIDENCE			x	x	x		x				
IA-12(3)	IDENTITY EVIDENCE VALIDATION AND VERIFICATION			x	x	x		x				
IA-12(5)	ADDRESS CONFIRMATION			x	x	x		x				

The following table includes additional regulatory controls for agencies with regulatory requirements

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
IA-2(5)	INDIVIDUAL AUTHENTICATION WITH GROUP AUTHENTICATION				x		x					x
IA-5(5)	CHANGE AUTHENTICATORS PRIOR TO DELIVERY					x						x
IA-5(7)	NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS					x	x					x

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
IA-2(6)	ACCESS TO ACCOUNTS — SEPARATE DEVICE					x						x
IA-2(10)	SINGLE SIGN-ON											
IA-2(13)	OUT-OF-BAND AUTHENTICATION											
IA-3(1)	CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION					x						
IA-3(3)	DYNAMIC ADDRESS ALLOCATION											
IA-3(4)	DEVICE ATTESTATION											
IA-4(1)	PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS											
IA-4(5)	DYNAMIC MANAGEMENT											
IA-4(6)	CROSS-ORGANIZATION MANAGEMENT											
IA-4(8)	PAIRWISE PSEUDONYMOUS IDENTIFIERS											
IA-4(9)	ATTRIBUTE MAINTENANCE AND PROTECTION											
IA-5(8)	MULTIPLE SYSTEM ACCOUNTS											
IA-5(9)	FEDERATED CREDENTIAL MANAGEMENT											
IA-5(10)	DYNAMIC CREDENTIAL BINDING											
IA-5(12)	BIOMETRIC AUTHENTICATION PERFORMANCE					x						
IA-5(13)	EXPIRATION OF CACHED AUTHENTICATORS											
IA-5(14)	MANAGING CONTENT OF PKI TRUST STORES											
IA-5(15)	GSA-APPROVED PRODUCTS AND SERVICES											
IA-5(16)	IN-PERSON OR TRUSTED EXTERNAL PARTY AUTHENTICATOR ISSUANCE											
IA-5(17)	PRESENTATION ATTACK DETECTION FOR BIOMETRIC AUTHENTICATORS											
IA-5(18)	PASSWORD MANAGERS											
IA-8(5)	ACCEPTANCE OF PIV-I CREDENTIALS											
IA-8(6)	DISASSOCIABILITY											
IA-9	Service Identification and Authentication					x					-	x
IA-10	Adaptive Authentication										-	
IA-12(4)	IN-PERSON VALIDATION AND VERIFICATION				x							x
IA-12(6)	ACCEPT EXTERNALLY-PROOFED IDENTITIES											

170 Incident Response Standard

The following table includes the baseline controls for the Incident Response Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
IR-1	Policy and Procedures	x	x	x	x	x	x	x			x	x
IR-2	Incident Response Training	x	x	x	x	x	x	x			x	x
IR-2(3)	BREACH	x				x		x				x
IR-3	Incident Response Testing	x		x	x	x	x	x	x		-	x
IR-3(2)	COORDINATION WITH RELATED PLANS			x	x	x	x	x				
IR-4	Incident Handling	x	x	x	x	x	x	x	x	x	x	x
IR-4(1)	AUTOMATED INCIDENT HANDLING PROCESSES			x	x	x	x	x				
IR-5	Incident Monitoring	x	x	x	x	x	x	x	x		-	
IR-6	Incident Reporting	x	x	x	x	x	x	x	x		x	x
IR-6(1)	AUTOMATED REPORTING			x	x	x	x	x				
IR-6(3)	SUPPLY CHAIN COORDINATION			x	x	x		x				
IR-7	Incident Response Assistance	x	x	x	x	x	x	x			-	
IR-7(1)	AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT			x	x	x	x	x				
IR-8	Incident Response Plan	x	x	x	x	x	x	x	x		x	x
IR-8(1)	BREACHES	x				x		x				

The following table includes additional regulatory controls for agencies with regulatory requirements

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
IR-6(2)	VULNERABILITIES RELATED TO INCIDENTS					x						x
IR-7(2)	COORDINATION WITH EXTERNAL PROVIDERS					x	x					
IR-9	Information Spillage Response					x	x				-	x

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
IR-2(1)	SIMULATED EVENTS				x	x						
IR-2(2)	AUTOMATED TRAINING ENVIRONMENTS				x							
IR-3(1)	AUTOMATED TESTING											
IR-3(3)	CONTINUOUS IMPROVEMENT					x						
IR-4(2)	DYNAMIC RECONFIGURATION											
IR-4(3)	CONTINUITY OF OPERATIONS											x
IR-4(4)	INFORMATION CORRELATION				x							x
IR-4(5)	AUTOMATIC DISABLING OF SYSTEM											
IR-4(6)	INSIDER THREATS					x						
IR-4(7)	INSIDER THREATS — INTRA-ORGANIZATION COORDINATION											
IR-4(8)	CORRELATION WITH EXTERNAL ORGANIZATIONS					x						
IR-4(9)	DYNAMIC RESPONSE CAPABILITY											
IR-4(10)	SUPPLY CHAIN COORDINATION											x
IR-4(11)	INTEGRATED INCIDENT RESPONSE TEAM				x							x
IR-4(12)	MALICIOUS CODE AND FORENSIC ANALYSIS											x
IR-4(13)	BEHAVIOR ANALYSIS											x
IR-4(14)	SECURITY OPERATIONS CENTER											
IR-4(15)	PUBLIC RELATIONS AND REPUTATION REPAIR											
IR-5(1)	AUTOMATED TRACKING, DATA COLLECTION, AND ANALYSIS				x							
IR-9(2)	TRAINING						x					
IR-9(3)	POST-SPILL OPERATIONS						x					x
IR-9(4)	EXPOSURE TO UNAUTHORIZED PERSONNEL						x					

180 System Maintenance Standard

The following table includes the baseline controls for the System Maintenance Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
MA-1	Policy and Procedures		x	x	x	x	x	x			x	x
MA-2	Controlled Maintenance		x	x	x	x	x	x	x		x	
MA-3	Maintenance Tools			x	x	x	x	x	x		-	
MA-3(1)	INSPECT TOOLS			x	x	x	x	x				
MA-3(2)	INSPECT MEDIA			x	x	x	x	x				
MA-3(3)	PREVENT UNAUTHORIZED REMOVAL			x	x	x	x	x				
MA-4	Nonlocal Maintenance		x	x	x	x	x	x	x		-	x
MA-5	Maintenance Personnel		x	x	x	x	x	x	x		-	
MA-6	Timely Maintenance			x	x	x	x	x			x	x

The following table includes additional regulatory controls for agencies with regulatory requirements

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
MA-4(1)	LOGGING AND REVIEW					x	x					x
MA-4(6)	CRYPTOGRAPHIC PROTECTION					x						x
MA-4(7)	DISCONNECT VERIFICATION					x						x

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
MA-2(2)	AUTOMATED MAINTENANCE ACTIVITIES				x							
MA-3(4)	RESTRICTED TOOL USE					x						
MA-3(5)	EXECUTION WITH PRIVILEGE					x						
MA-3(6)	SOFTWARE UPDATES AND PATCHES											
MA-4(3)	COMPARABLE SECURITY AND SANITIZATION				x							
MA-4(4)	AUTHENTICATION AND SEPARATION OF MAINTENANCE SESSIONS					x						
MA-4(5)	APPROVALS AND NOTIFICATIONS											
MA-5(1)	INDIVIDUALS WITHOUT APPROPRIATE ACCESS				x		x					
MA-5(2)	SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS											
MA-5(3)	CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS											
MA-5(4)	FOREIGN NATIONALS											
MA-5(5)	NON-SYSTEM MAINTENANCE					x						
MA-6(1)	PREVENTIVE MAINTENANCE											
MA-6(2)	PREDICTIVE MAINTENANCE											
MA-6(3)	AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE											
MA-7	Field Maintenance										-	

190 Media Protection Standard

The following table includes the baseline controls for the Media Protection Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
MP-1	Policy and Procedures	x	x	x	x	x	x	x			x	x
MP-2	Media Access		x	x	x	x	x	x	x		x	x
MP-3	Media Marking			x	x	x	x				x	
MP-4	Media Storage			x	x	x	x	x	x		x	x
MP-5	Media Transport			x	x	x	x	x	x		x	x
MP-6	Media Sanitization	x	x	x	x	x	x	x	x		x	x
MP-6(1)	REVIEW, APPROVE, TRACK, DOCUMENT, AND VERIFY				x	x	x					x
MP-7	Media Use		x	x	x	x	x	x	x		x	x

The following table includes additional regulatory controls for agencies with regulatory requirements

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
MP-6(2)	EQUIPMENT TESTING				x		x					

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
MP-4(2)	AUTOMATED RESTRICTED ACCESS											
MP-5(3)	CUSTODIANS					x						x
MP-6(3)	NONDESTRUCTIVE TECHNIQUES				x							x
MP-6(7)	DUAL AUTHORIZATION											
MP-6(8)	REMOTE PURGING OR WIPING OF INFORMATION											
MP-7(2)	PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA											
MP-8	Media Downgrading										-	
MP-8(1)	DOCUMENTATION OF PROCESS											
MP-8(2)	EQUIPMENT TESTING											
MP-8(3)	CONTROLLED UNCLASSIFIED INFORMATION											
MP-8(4)	CLASSIFIED INFORMATION											

200 Physical and Environment Protection Standard

The following table includes the baseline controls for the Physical and Environment Protection Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
PE-1	Policy and Procedures		x	x	x	x	x	x			x	x
PE-2	Physical Access Authorizations		x	x	x	x	x	x	x		x	x
PE-3	Physical Access Control		x	x	x	x	x	x	x	x	x	x
PE-4	Access Control for Transmission			x	x	x	x	x	x		x	x
PE-5	Access Control for Output Devices			x	x	x	x	x	x		x	x
PE-6	Monitoring Physical Access		x	x	x	x	x	x	x	x	-	x
PE-6(1)	INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT			x	x	x	x	x				x
PE-8	Visitor Access Records		x	x	x	x	x	x			-	x
PE-8(3)	LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	x						x				x
PE-9	Power Equipment and Cabling			x	x		x	x	x		x	
PE-10	Emergency Shutoff			x	x		x	x	x		x	
PE-11	Emergency Power			x	x		x	x	x		x	
PE-12	Emergency Lighting		x	x	x		x	x	x		x	
PE-13	Fire Protection		x	x	x		x	x	x		x	
PE-13(1)	DETECTION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION			x	x			x				
PE-14	Environmental Controls		x	x	x		x	x	x		x	
PE-15	Water Damage Protection		x	x	x		x	x	x		x	
PE-16	Delivery and Removal		x	x	x	x	x	x	x		x	
PE-17	Alternate Work Site			x	x	x	x	x			x	

The following table includes additional regulatory controls for agencies with regulatory requirements

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
PE-2(1)	ACCESS BY POSITION AND ROLE						x					x

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
PE-2(2)	TWO FORMS OF IDENTIFICATION											x
PE-2(3)	RESTRICT UNESCORTED ACCESS											x
PE-3(1)	SYSTEM ACCESS				x							
PE-3(2)	FACILITY AND SYSTEMS					x						x
PE-3(3)	CONTINUOUS GUARDS											x
PE-3(4)	LOCKABLE CASINGS											x
PE-3(5)	TAMPER PROTECTION											
PE-3(7)	PHYSICAL BARRIERS											
PE-3(8)	ACCESS CONTROL VESTIBULES											
PE-5(2)	LINK TO INDIVIDUAL IDENTITY											
PE-6(2)	AUTOMATED INTRUSION RECOGNITION AND RESPONSES											
PE-6(3)	VIDEO SURVEILLANCE											
PE-6(4)	MONITORING PHYSICAL ACCESS TO SYSTEMS				x							x
PE-8(1)	AUTOMATED RECORDS MAINTENANCE AND REVIEW				x							x
PE-9(1)	REDUNDANT CABLING											
PE-9(2)	AUTOMATIC VOLTAGE CONTROLS											
PE-11(1)	ALTERNATE POWER SUPPLY — MINIMAL OPERATIONAL CAPABILITY				x							
PE-11(2)	ALTERNATE POWER SUPPLY — SELF-CONTAINED											
PE-12(1)	ESSENTIAL MISSIONS AND BUSINESS FUNCTIONS											
PE-13(2)	SUPPRESSION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION				x							
PE-13(4)	INSPECTIONS											
PE-14(1)	AUTOMATIC CONTROLS											
PE-14(2)	MONITORING WITH ALARMS AND NOTIFICATIONS											
PE-15(1)	AUTOMATION SUPPORT				x							
PE-18	Location of System Components				x				x		x	x
PE-19	Information Leakage								x		x	
PE-19(1)	NATIONAL EMISSIONS POLICIES AND PROCEDURES											
PE-20	Asset Monitoring and Tracking								x		x	
PE-21	Electromagnetic Pulse Protection										-	
PE-22	Component Marking										x	x
PE-23	Facility Location										x	x

210 Security Planning Standard

The following table includes the baseline controls for the Security Planning Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
PL-1	Policy and Procedures	x	x	x	x	x	x	x		x	x	x
PL-2	System Security and Privacy Plans	x	x	x	x	x	x	x	x		x	x
PL-4	Rules of Behavior	x	x	x	x	x	x	x		x	x	x
PL-4(1)	SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS	x	x	x	x	x	x	x				
PL-8	Security and Privacy Architectures	x		x	x	x	x	x	x		x	x
PL-9	Central Management	x						x			-	x
PL-10	Baseline Selection		x	x	x			x			-	x
PL-11	Baseline Tailoring		x	x	x			x			-	

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
PL-7	Concept of Operations										x	
PL-8(1)	DEFENSE IN DEPTH					x						x
PL-8(2)	SUPPLIER DIVERSITY											

220 Personnel Security Standard

The following table includes the baseline controls for the Personnel Security Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
PS-1	Policy and Procedures		x	x	x	x	x	x	x		x	x
PS-2	Position Risk Designation		x	x	x	x	x	x	x		-	x
PS-3	Personnel Screening		x	x	x	x	x	x	x	x	x	x
PS-4	Personnel Termination		x	x	x	x	x	x	x		x	x
PS-5	Personnel Transfer		x	x	x	x	x	x	x		x	
PS-6	Access Agreements	x	x	x	x	x	x	x	x	x	x	
PS-7	External Personnel Security		x	x	x	x	x	x	x		x	
PS-8	Personnel Sanctions		x	x	x	x	x	x	x		x	
PS-9	Position Descriptions		x	x	x	x		x			x	x

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
PS-3(1)	CLASSIFIED INFORMATION											x
PS-3(2)	FORMAL INDOCTRINATION											
PS-3(3)	INFORMATION REQUIRING SPECIAL PROTECTION MEASURES											x
PS-3(4)	CITIZENSHIP REQUIREMENTS											
PS-4(1)	POST-EMPLOYMENT REQUIREMENTS											
PS-4(2)	AUTOMATED ACTIONS				x							
PS-6(2)	CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION											
PS-6(3)	POST-EMPLOYMENT REQUIREMENTS					x						

230 Risk Assessment Standard

The following table includes the baseline controls for the Risk Assessment Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
RA-1	Policy and Procedures	x	x	x	x	x	x	x			x	x
RA-2	Security Categorization		x	x	x		x	x	x		x	x
RA-3	Risk Assessment	x	x	x	x	x	x	x	x		x	x
RA-3(1)	SUPPLY CHAIN RISK ASSESSMENT		x	x	x	x						
RA-5	Vulnerability Monitoring and Scanning		x	x	x	x	x	x	x	x	x	x
RA-5(2)	UPDATE VULNERABILITIES TO BE SCANNED		x	x	x	x	x	x				x
RA-5(5)	PRIVILEGED ACCESS			x	x	x	x	x				
RA-5(11)	PUBLIC DISCLOSURE PROGRAM		x	x	x			x				x
RA-7	Risk Response	x	x	x	x	x		x			x	x
RA-8	Privacy Impact Assessments	x				x					-	x
RA-9	Criticality Analysis			x	x			x			x	x

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
RA-2(1)	IMPACT-LEVEL PRIORITIZATION											
RA-3(2)	USE OF ALL-SOURCE INTELLIGENCE											
RA-3(3)	DYNAMIC THREAT AWARENESS											
RA-3(4)	PREDICTIVE CYBER ANALYTICS											
RA-5(3)	BREADTH AND DEPTH OF COVERAGE						x					x
RA-5(4)	DISCOVERABLE INFORMATION				x	x						x
RA-5(6)	AUTOMATED TREND ANALYSES						x					
RA-5(8)	REVIEW HISTORIC AUDIT LOGS						x					
RA-5(10)	CORRELATE SCANNING INFORMATION											
RA-6	Technical Surveillance Countermeasures Survey										-	
RA-10	Threat Hunting											

240 System and Services Acquisition Standard

The following table includes the baseline controls for the System and Services Acquisition Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
SA-1	Policy and Procedures	x	x	x	x	x	x	x			x	x
SA-2	Allocation of Resources	x	x	x	x	x	x	x			-	
SA-3	System Development Life Cycle	x	x	x	x	x	x	x	x		x	x
SA-4	Acquisition Process	x	x	x	x	x	x	x	x		x	x
SA-4(1)	FUNCTIONAL PROPERTIES OF CONTROLS			x	x	x	x	x				x
SA-4(2)	DESIGN AND IMPLEMENTATION INFORMATION FOR CONTROLS			x	x	x	x	x				x
SA-4(9)	FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES IN USE			x	x	x	x	x				x
SA-4(10)	USE OF APPROVED PIV PRODUCTS		x	x	x			x				
SA-5	System Documentation		x	x	x	x	x	x	x		x	x
SA-8	Security and Privacy Engineering Principles		x	x	x	x	x	x	x		x	x
SA-8(33)	MINIMIZATION	x						x				x
SA-9	External System Services	x	x	x	x	x	x	x	x		x	x
SA-9(2)	IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES			x	x	x	x	x				x
SA-10	Developer Configuration Management			x	x	x	x	x	x		x	
SA-11	Developer Testing and Evaluation	x		x	x	x	x	x	x		x	x
SA-15	Development Process, Standards, and Tools			x	x	x		x	x		x	x
SA-15(3)	CRITICALITY ANALYSIS			x	x	x		x				
SA-22	Unsupported System Components		x	x	x	x	x	x			-	

The following table includes additional regulatory controls for agencies with regulatory requirements

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
SA-4(8)	CONTINUOUS MONITORING PLAN FOR CONTROLS					x	x					
SA-9(1)	RISK ASSESSMENTS AND ORGANIZATIONAL APPROVALS					x	x					x
SA-9(5)	PROCESSING, STORAGE, AND SERVICE LOCATION					x	x					x
SA-10(1)	SOFTWARE AND FIRMWARE INTEGRITY VERIFICATION					x	x					
SA-11(1)	STATIC CODE ANALYSIS					x	x					x

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
SA-3(1)	MANAGE PREPRODUCTION ENVIRONMENT											x
SA-3(2)	USE OF LIVE OR OPERATIONAL DATA					x						x
SA-3(3)	TECHNOLOGY REFRESH											x
SA-4(3)	DEVELOPMENT METHODS, TECHNIQUES, AND PRACTICES											x
SA-4(5)	SYSTEM, COMPONENT, AND SERVICE CONFIGURATIONS				x							
SA-4(6)	USE OF INFORMATION ASSURANCE PRODUCTS											
SA-4(7)	NIAP-APPROVED PROTECTION PROFILES											
SA-4(11)	SYSTEM OF RECORDS											
SA-4(12)	DATA OWNERSHIP					x						x
SA-8(1)	CLEAR ABSTRACTIONS											
SA-8(2)	LEAST COMMON MECHANISM											
SA-8(3)	MODULARITY AND LAYERING											
SA-8(4)	PARTIALLY ORDERED DEPENDENCIES											
SA-8(5)	EFFICIENTLY MEDIATED ACCESS											
SA-8(6)	MINIMIZED SHARING											
SA-8(7)	REDUCED COMPLEXITY											
SA-8(8)	SECURE EVOLVABILITY											
SA-8(9)	TRUSTED COMPONENTS											
SA-8(10)	HIERARCHICAL TRUST											
SA-8(11)	INVERSE MODIFICATION THRESHOLD											
SA-8(12)	HIERARCHICAL PROTECTION											
SA-8(13)	MINIMIZED SECURITY ELEMENTS											
SA-8(14)	LEAST PRIVILEGE											x
SA-8(15)	PREDICATE PERMISSION											
SA-8(16)	SELF-RELIANT TRUSTWORTHINESS											
SA-8(17)	SECURE DISTRIBUTED COMPOSITION											
SA-8(18)	TRUSTED COMMUNICATIONS CHANNELS											
SA-8(19)	CONTINUOUS PROTECTION											
SA-8(20)	SECURE METADATA MANAGEMENT											
SA-8(21)	SELF-ANALYSIS											
SA-8(22)	ACCOUNTABILITY AND TRACEABILITY											
SA-8(23)	SECURE DEFAULTS											
SA-8(24)	SECURE FAILURE AND RECOVERY											
SA-8(25)	ECONOMIC SECURITY											
SA-8(26)	PERFORMANCE SECURITY											
SA-8(27)	HUMAN FACTORED SECURITY											
SA-8(28)	ACCEPTABLE SECURITY											
SA-8(29)	REPEATABLE AND DOCUMENTED PROCEDURES											
SA-8(30)	PROCEDURAL RIGOR											x
SA-8(31)	SECURE SYSTEM MODIFICATION											x
SA-8(32)	SUFFICIENT DOCUMENTATION											x
SA-9(3)	ESTABLISH AND MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS					x						x
SA-9(4)	CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS											
SA-9(6)	ORGANIZATION-CONTROLLED CRYPTOGRAPHIC KEYS					x						
SA-9(7)	ORGANIZATION-CONTROLLED INTEGRITY CHECKING											
SA-9(8)	PROCESSING AND STORAGE LOCATION — U.S. JURISDICTION					x						
SA-10(2)	ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES											
SA-10(3)	HARDWARE INTEGRITY VERIFICATION					x						
SA-10(4)	TRUSTED GENERATION											
SA-10(5)	MAPPING INTEGRITY FOR VERSION CONTROL											
SA-10(6)	TRUSTED DISTRIBUTION											
SA-10(7)	SECURITY AND PRIVACY REPRESENTATIVES					x						
SA-11(2)	THREAT MODELING AND VULNERABILITY ANALYSES						x					x
SA-11(3)	INDEPENDENT VERIFICATION OF ASSESSMENT PLANS AND EVIDENCE											
SA-11(4)	MANUAL CODE REVIEWS					x						
SA-11(5)	PENETRATION TESTING					x						x
SA-11(6)	ATTACK SURFACE REVIEWS					x						x
SA-11(7)	VERIFY SCOPE OF TESTING AND EVALUATION											x
SA-11(8)	DYNAMIC CODE ANALYSIS						x					x
SA-11(9)	INTERACTIVE APPLICATION SECURITY TESTING											

SA-15(1)	QUALITY METRICS							x				
SA-15(2)	SECURITY AND PRIVACY TRACKING TOOLS											
SA-15(5)	ATTACK SURFACE REDUCTION											x
SA-15(6)	CONTINUOUS IMPROVEMENT											
SA-15(7)	AUTOMATED VULNERABILITY ANALYSIS											
SA-15(8)	REUSE OF THREAT AND VULNERABILITY INFORMATION											
SA-15(10)	INCIDENT RESPONSE PLAN											
SA-15(11)	ARCHIVE SYSTEM OR COMPONENT											
SA-15(12)	MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION											
SA-16	Developer-Provided Training				x						-	
SA-17	Developer Security and Privacy Architecture and Design				x				x		x	x
SA-17(1)	FORMAL POLICY MODEL											
SA-17(2)	SECURITY-RELEVANT COMPONENTS											
SA-17(3)	FORMAL CORRESPONDENCE											
SA-17(4)	INFORMAL CORRESPONDENCE											
SA-17(5)	CONCEPTUALLY SIMPLE DESIGN											
SA-17(6)	STRUCTURE FOR TESTING											
SA-17(7)	STRUCTURE FOR LEAST PRIVILEGE											
SA-17(8)	ORCHESTRATION											
SA-17(9)	DESIGN DIVERSITY											
SA-20	Customized Development of Critical Components										-	
SA-21	Developer Screening				x						x	x
SA-23	Specialization										-	x

250 System and Communications Protection Standard

The following table includes the baseline controls for the System and Communications Protection Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
SC-1	Policy and Procedures		x	x	x	x	x	x			x	x
SC-2	Separation of System and User Functionality			x	x	x	x	x			-	
SC-4	Information in Shared System Resources			x	x	x	x	x			-	
SC-5	Denial-of-Service Protection		x	x	x		x	x	x		-	
SC-7	Boundary Protection		x	x	x	x	x	x	x	x	x	x
SC-7(3)	ACCESS POINTS			x	x	x	x	x				x
SC-7(4)	EXTERNAL TELECOMMUNICATIONS SERVICES			x	x	x	x	x				
SC-7(5)	DENY BY DEFAULT — ALLOW BY EXCEPTION			x	x	x	x	x				x
SC-7(7)	SPLIT TUNNELING FOR REMOTE DEVICES			x	x	x	x	x				x
SC-7(8)	ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS			x	x	x	x	x				
SC-7(24)	PERSONALLY IDENTIFIABLE INFORMATION	x						x				
SC-8	Transmission Confidentiality and Integrity			x	x	x	x	x	x		x	x
SC-8(1)	CRYPTOGRAPHIC PROTECTION			x	x	x	x	x				x
SC-10	Network Disconnect			x	x	x	x	x			x	x
SC-12	Cryptographic Key Establishment and Management		x	x	x	x	x	x			x	
SC-13	Cryptographic Protection		x	x	x	x	x	x	x		x	x
SC-15	Collaborative Computing Devices and Applications		x	x	x	x	x	x			x	
SC-17	Public Key Infrastructure Certificates			x	x	x	x	x			x	
SC-18	Mobile Code			x	x	x	x	x	x		-	
SC-20	Secure Name/Address Resolution Service (Authoritative Source)		x	x	x	x	x	x			-	
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)		x	x	x	x	x	x			-	
SC-22	Architecture and Provisioning for Name/Address Resolution Service		x	x	x	x	x	x			-	
SC-23	Session Authenticity			x	x	x	x	x			-	x
SC-28	Protection of Information at Rest			x	x	x	x	x	x		x	x
SC-28(1)	CRYPTOGRAPHIC PROTECTION			x	x	x	x	x				x
SC-39	Process Isolation		x	x	x	x	x	x			-	

The following table includes additional regulatory controls for agencies with regulatory requirements

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
SC-2(1)	INTERFACES FOR NON-PRIVILEGED USERS					x						
SC-6	Resource Availability						x				-	
SC-7(11)	RESTRICT INCOMING COMMUNICATIONS TRAFFIC					x						x
SC-7(12)	HOST-BASED PROTECTION					x	x					x
SC-7(13)	ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS						x					
SC-7(18)	FAIL SECURE				x	x	x					x
SC-8(2)	PRE- AND POST-TRANSMISSION HANDLING						x					x
SC-12(2)	SYMMETRIC KEYS						x					
SC-12(3)	ASYMMETRIC KEYS						x					
SC-18(1)	IDENTIFY UNACCEPTABLE CODE AND TAKE CORRECTIVE ACTIONS					x						x
SC-18(2)	ACQUISITION, DEVELOPMENT, AND USE					x						
SC-23(1)	INVALIDATE SESSION IDENTIFIERS AT LOGOUT					x						
SC-23(3)	UNIQUE SYSTEM-GENERATED SESSION IDENTIFIERS					x						
SC-32	System Partitioning						x				-	

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
SC-2(2)	DISASSOCIABILITY											
SC-3	Security Function Isolation				x						-	x
SC-3(1)	HARDWARE SEPARATION											
SC-3(2)	ACCESS AND FLOW CONTROL FUNCTIONS											
SC-3(3)	MINIMIZE NONSECURITY FUNCTIONALITY											
SC-3(4)	MODULE COUPLING AND COHESIVENESS											
SC-3(5)	LAYERED STRUCTURES											x
SC-4(2)	MULTILEVEL OR PERIODS PROCESSING											
SC-5(1)	RESTRICT ABILITY TO ATTACK OTHER SYSTEMS											
SC-5(2)	CAPACITY, BANDWIDTH, AND REDUNDANCY											
SC-5(3)	DETECTION AND MONITORING											
SC-7(9)	RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC					x						x
SC-7(10)	PREVENT EXFILTRATION					x						x
SC-7(14)	PROTECT AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS											x
SC-7(15)	NETWORKED PRIVILEGED ACCESSES					x						
SC-7(16)	PREVENT DISCOVERY OF SYSTEM COMPONENTS											x
SC-7(17)	AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS					x						x
SC-7(19)	BLOCK COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS											
SC-7(20)	DYNAMIC ISOLATION AND SEGREGATION											
SC-7(21)	ISOLATION OF SYSTEM COMPONENTS				x							x
SC-7(22)	SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS											x
SC-7(23)	DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE											
SC-7(25)	UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS											
SC-7(26)	CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS											
SC-7(27)	UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS											x
SC-7(28)	CONNECTIONS TO PUBLIC NETWORKS											
SC-7(29)	SEPARATE SUBNETS TO ISOLATE FUNCTIONS											x
SC-8(3)	CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS											
SC-8(4)	CONCEAL OR RANDOMIZE COMMUNICATIONS											
SC-8(5)	PROTECTED DISTRIBUTION SYSTEM											
SC-11	Trusted Path										-	
SC-11(1)	IRREFUTABLE COMMUNICATIONS PATH											
SC-12(1)	AVAILABILITY				x							x
SC-12(6)	PHYSICAL CONTROL OF KEYS											
SC-15(1)	PHYSICAL OR LOGICAL DISCONNECT											
SC-15(3)	DISABLING AND REMOVAL IN SECURE WORK AREAS											
SC-15(4)	EXPLICITLY INDICATE CURRENT PARTICIPANTS					x						
SC-16	Transmission of Security and Privacy Attributes										-	
SC-16(1)	INTEGRITY VERIFICATION											x
SC-16(2)	ANTI-SPOOFING MECHANISMS											
SC-16(3)	CRYPTOGRAPHIC BINDING											
SC-18(3)	PREVENT DOWNLOADING AND EXECUTION											
SC-18(4)	PREVENT AUTOMATIC EXECUTION											
SC-18(5)	ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS											
SC-20(2)	DATA ORIGIN AND INTEGRITY					x						
SC-23(5)	ALLOWED CERTIFICATE AUTHORITIES					x						
SC-24	Fail in Known State				x						-	
SC-25	Thin Nodes										-	
SC-26	Decoys										-	
SC-27	Platform-Independent Applications										-	
SC-28(2)	OFFLINE STORAGE											x
SC-28(3)	CRYPTOGRAPHIC KEYS											x
SC-29	Heterogeneity										-	
SC-29(1)	VIRTUALIZATION TECHNIQUES											
SC-30	Concealment and Misdirection										-	
SC-30(2)	RANDOMNESS											
SC-30(3)	CHANGE PROCESSING AND STORAGE LOCATIONS											
SC-30(4)	MISLEADING INFORMATION											
SC-30(5)	CONCEALMENT OF SYSTEM COMPONENTS											
SC-31	Covert Channel Analysis								x		-	x
SC-31(1)	TEST COVERT CHANNELS FOR EXPLOITABILITY											
SC-31(2)	MAXIMUM BANDWIDTH											
SC-31(3)	MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS											
SC-32(1)	SEPARATE PHYSICAL DOMAINS FOR PRIVILEGED FUNCTIONS											
SC-34	Non-Modifiable Executable Programs										-	
SC-34(1)	NO WRITABLE STORAGE											
SC-34(2)	INTEGRITY PROTECTION AND READ-ONLY MEDIA											
SC-35	External Malicious Code Identification					x					-	
SC-36	Distributed Processing and Storage										-	
SC-36(1)	POLLING TECHNIQUES											
SC-36(2)	SYNCHRONIZATION											

SC-37	Out-of-Band Channels										-	
SC-37(1)	ENSURE DELIVERY AND TRANSMISSION											
SC-38	Operations Security										x	x
SC-39(1)	HARDWARE SEPARATION											
SC-39(2)	SEPARATE EXECUTION DOMAIN PER THREAD											
SC-40	Wireless Link Protection										-	x
SC-40(1)	ELECTROMAGNETIC INTERFERENCE											
SC-40(2)	REDUCE DETECTION POTENTIAL											
SC-40(3)	IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION											
SC-40(4)	SIGNAL PARAMETER IDENTIFICATION											
SC-41	Port and I/O Device Access										-	
SC-42	Sensor Capability and Data										x	
SC-42(1)	REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES											
SC-42(2)	AUTHORIZED USE											
SC-42(4)	NOTICE OF COLLECTION											
SC-42(5)	COLLECTION MINIMIZATION											
SC-43	Usage Restrictions										-	
SC-44	Detonation Chambers								x		-	
SC-45	System Time Synchronization					x					-	x
SC-45(1)	SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE					x						x
SC-45(2)	SECONDARY AUTHORITATIVE TIME SOURCE											
SC-46	Cross Domain Policy Enforcement										-	
SC-47	Alternate Communications Paths										-	
SC-48	Sensor Relocation										-	x
SC-48(1)	DYNAMIC RELOCATION OF SENSORS OR MONITORING CAPABILITIES											
SC-49	Hardware-Enforced Separation and Policy Enforcement										-	
SC-50	Software-Enforced Separation and Policy Enforcement										-	
SC-51	Hardware-Based Protection										-	

260 System and Information Integrity Standard

The following table includes the baseline controls for the System and Information Integrity Standard

CONTROL NUMBER	**CONTROL NAME** CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
SI-1	Policy and Procedures	x	x	x	x	x	x	x			x	x
SI-2	Flaw Remediation		x	x	x	x	x	x	x	x	x	x
SI-2(2)	AUTOMATED FLAW REMEDIATION STATUS			x	x	x	x	x				
SI-3	Malicious Code Protection		x	x	x	x	x	x	x		x	x
SI-4	System Monitoring		x	x	x	x	x	x	x	x	-	x
SI-4(2)	AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS			x	x	x	x	x				x
SI-4(4)	INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC			x	x	x	x	x				
SI-4(5)	SYSTEM-GENERATED ALERTS			x	x	x	x	x				x
SI-5	Security Alerts, Advisories, and Directives		x	x	x	x	x	x	x		x	x
SI-7	Software, Firmware, and Information Integrity			x	x	x	x	x	x		-	x
SI-7(1)	INTEGRITY CHECKS			x	x	x	x	x				
SI-7(7)	INTEGRATION OF DETECTION AND RESPONSE			x	x	x	x	x				x
SI-8	Spam Protection			x	x	x	x	x			-	x
SI-8(2)	AUTOMATIC UPDATES			x	x	x	x	x				
SI-10	Information Input Validation			x	x	x	x	x			-	
SI-11	Error Handling			x	x	x	x	x			-	
SI-12	Information Management and Retention	x	x	x	x	x	x	x			-	x
SI-12(1)	LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	x						x				x
SI-12(2)	MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH	x				x		x				x
SI-12(3)	INFORMATION DISPOSAL	x						x				x
SI-16	Memory Protection			x	x	x	x	x			-	
SI-18	Personally Identifiable Information Quality Operations	x									-	
SI-18(4)	INDIVIDUAL REQUESTS	x										
SI-19	De-identification	x									-	

The following table includes additional regulatory controls for agencies with regulatory requirements

CONTROL NUMBER	**CONTROL NAME** CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
SI-2(3)	TIME TO REMEDIATE FLAWS AND BENCHMARKS FOR CORRECTIVE ACTIONS					x						
SI-4(1)	SYSTEM-WIDE INTRUSION DETECTION SYSTEM					x	x					x
SI-4(11)	ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES					x						x
SI-4(12)	AUTOMATED ORGANIZATION-GENERATED ALERTS				x	x						
SI-4(14)	WIRELESS INTRUSION DETECTION				x		x					x

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	HIPAA Security Rule 45 C.F.R	FERPA	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH							
SI-2(4)	AUTOMATED PATCH MANAGEMENT TOOLS					x						x
SI-2(5)	AUTOMATIC SOFTWARE AND FIRMWARE UPDATES					x						
SI-2(6)	REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE AND FIRMWARE					x						
SI-3(4)	UPDATES ONLY BY PRIVILEGED USERS											
SI-3(6)	TESTING AND VERIFICATION											
SI-3(8)	DETECT UNAUTHORIZED COMMANDS											
SI-3(10)	MALICIOUS CODE ANALYSIS											
SI-4(3)	AUTOMATED TOOL AND MECHANISM INTEGRATION											
SI-4(7)	AUTOMATED RESPONSE TO SUSPICIOUS EVENTS											
SI-4(9)	TESTING OF MONITORING TOOLS AND MECHANISMS											x
SI-4(10)	VISIBILITY OF ENCRYPTED COMMUNICATIONS				x	x						
SI-4(13)	ANALYZE TRAFFIC AND EVENT PATTERNS											
SI-4(15)	WIRELESS TO WIRELINE COMMUNICATIONS											x
SI-4(16)	CORRELATE MONITORING INFORMATION						x					x
SI-4(17)	INTEGRATED SITUATIONAL AWARENESS											
SI-4(18)	ANALYZE TRAFFIC AND COVERT EXFILTRATION					x						x
SI-4(19)	RISK FOR INDIVIDUALS											
SI-4(20)	PRIVILEGED USERS				x							
SI-4(21)	PROBATIONARY PERIODS											
SI-4(22)	UNAUTHORIZED NETWORK SERVICES				x							
SI-4(23)	HOST-BASED DEVICES						x					
SI-4(24)	INDICATORS OF COMPROMISE					x						x
SI-4(25)	OPTIMIZE NETWORK TRAFFIC ANALYSIS											x
SI-5(1)	AUTOMATED ALERTS AND ADVISORIES				x							x
SI-6	Security and Privacy Function Verification				x		x				-	x
SI-6(2)	AUTOMATION SUPPORT FOR DISTRIBUTED TESTING											
SI-6(3)	REPORT VERIFICATION RESULTS											x
SI-7(2)	AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS				x							
SI-7(3)	CENTRALLY MANAGED INTEGRITY TOOLS											
SI-7(5)	AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS				x							
SI-7(6)	CRYPTOGRAPHIC PROTECTION											x
SI-7(8)	AUDITING CAPABILITY FOR SIGNIFICANT EVENTS											
SI-7(9)	VERIFY BOOT PROCESS											
SI-7(10)	PROTECTION OF BOOT FIRMWARE					x						
SI-7(12)	INTEGRITY VERIFICATION											
SI-7(15)	CODE AUTHENTICATION				x							
SI-7(16)	TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION											
SI-7(17)	RUNTIME APPLICATION SELF-PROTECTION											
SI-8(3)	CONTINUOUS LEARNING CAPABILITY											
SI-10(1)	MANUAL OVERRIDE CAPABILITY											
SI-10(2)	REVIEW AND RESOLVE ERRORS											
SI-10(3)	PREDICTABLE BEHAVIOR											
SI-10(4)	TIMING INTERACTIONS											
SI-10(5)	RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS											
SI-10(6)	INJECTION PREVENTION											
SI-13	Predictable Failure Prevention										-	
SI-13(1)	TRANSFERRING COMPONENT RESPONSIBILITIES											
SI-13(3)	MANUAL TRANSFER BETWEEN COMPONENTS											
SI-13(4)	STANDBY COMPONENT INSTALLATION AND NOTIFICATION											
SI-13(5)	FAILOVER CAPABILITY											
SI-14	Non-Persistence										-	
SI-14(1)	REFRESH FROM TRUSTED SOURCES											
SI-14(2)	NON-PERSISTENT INFORMATION											
SI-14(3)	NON-PERSISTENT CONNECTIVITY											
SI-15	Information Output Filtering										-	
SI-17	Fail-Safe Procedures										-	
SI-18(1)	AUTOMATION SUPPORT											
SI-18(2)	DATA TAGS											
SI-18(3)	COLLECTION											
SI-18(5)	NOTICE OF CORRECTION OR DELETION											
SI-19(1)	COLLECTION											
SI-19(2)	ARCHIVING											
SI-19(3)	RELEASE											
SI-19(4)	REMOVAL, MASKING, ENCRYPTION, HASHING, OR REPLACEMENT OF DIRECT IDENTIFIERS											x
SI-19(5)	STATISTICAL DISCLOSURE CONTROL											
SI-19(6)	DIFFERENTIAL PRIVACY											
SI-19(7)	VALIDATED ALGORITHMS AND SOFTWARE											
SI-19(8)	MOTIVATED INTRUDER											
SI-20	Tainting										-	
SI-21	Information Refresh										-	
SI-22	Information Diversity										-	
SI-23	Information Fragmentation										-	

270 PII and Transparency Standard

The following table includes the baseline controls for the PII and Transparency Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH					
PT-1	Policy and Procedures	x				x			-	x
PT-2	Authority to Process Personally Identifiable Information	x				x			-	x
PT-3	Personally Identifiable Information Processing Purposes	x							-	x
PT-4	Consent	x							-	
PT-5	Privacy Notice	x							-	
PT-7	Specific Categories of Personally Identifiable Information	x							-	x
PT-7(1)	SOCIAL SECURITY NUMBERS	x								
PT-7(2)	FIRST AMENDMENT INFORMATION	x								

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL	SECURITY CONTROL			IRS Publication	MARS-E 2.2	CJIS 6.0	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH					
PT-2(1)	DATA TAGGING									
PT-2(2)	AUTOMATION									
PT-3(1)	DATA TAGGING									
PT-3(2)	AUTOMATION									
PT-4(1)	TAILORED CONSENT									
PT-4(2)	JUST-IN-TIME CONSENT									
PT-4(3)	REVOCATION									
PT-5(1)	JUST-IN-TIME NOTICE									
PT-5(2)	PRIVACY ACT STATEMENTS	x								
PT-6	System of Records Notice	x							-	
PT-6(1)	ROUTINE USES	x								
PT-6(2)	EXEMPTION RULES	x								
PT-8	Computer Matching Requirements	x							-	

280 Supply Chain Risk Management Standard

The following table includes the baseline controls for the Supply Chain Risk Management Standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH					
SR-1	Policy and Procedures		x	x	x	x		x	x	x
SR-2	Supply Chain Risk Management Plan		x	x	x	x		x	x	
SR-3	Supply Chain Controls and Processes		x	x	x	x			x	
SR-5	Acquisition Strategies, Tools, and Methods		x	x	x			x	x	
SR-6	Supplier Assessments and Reviews			x	x	x			x	x
SR-8	Notification Agreements		x	x	x			x	-	
SR-10	Inspection of Systems or Components		x	x	x	x		x	-	x
SR-11	Component Authenticity		x	x	x	x			-	
SR-11(1)	ANTI-COUNTERFEIT TRAINING		x	x	x	x				
SR-11(2)	CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR		x	x	x	x				
SR-12	COMPONENT DISPOSAL		x	x	x			x	-	x

The following controls were not selected to be included in the standard

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL			IRS Publication 1075	MARS-E 2.2	CJIS 6.0	ISO 270001	PCI-DSS v4.0.1
			LOW	MOD	HIGH					
SR-2(1)	ESTABLISH SCRM TEAM		x	x	x	x		x		
SR-3(1)	DIVERSE SUPPLY BASE									x
SR-3(2)	LIMITATION OF HARM					x				
SR-3(3)	SUB-TIER FLOW DOWN					x				x
SR-4	Provenance								x	
SR-4(1)	IDENTITY									
SR-4(2)	TRACK AND TRACE									
SR-4(3)	VALIDATE AS GENUINE AND NOT ALTERED									
SR-4(4)	SUPPLY CHAIN INTEGRITY — PEDIGREE									
SR-5(1)	ADEQUATE SUPPLY									

SR-5(2)	ASSESSMENTS PRIOR TO SELECTION, ACCEPTANCE, MODIFICATION, OR UPDATE									
SR-6(1)	TESTING AND ANALYSIS									x
SR-7	Supply Chain Operations Security								x	x
SR-9	Tamper Resistance and Detection				x				-	x
SR-9(1)	MULTIPLE STAGES OF SYSTEM DEVELOPMENT LIFE CYCLE				x					
SR-11(3)	ANTI-COUNTERFEIT SCANNING									

500 Program Management Standard

The following table includes the baseline controls in the Program Management Standard

CONTROL	CONTROL NAME	PRIVACY	SECURITY CONTROL			IRS Publication	MARS-E	CJIS 6.0	HIPAA Security	FERPA	ISO	PCI-DSS
NUMBER	CONTROL ENHANCEMENT NAME	CONTROL	LOW	MOD	HIGH	1075	2.2		Rule 45 C.F.R		270001	v4.0.1
PM-1	Information Security Program Plan					x	x		x		x	x
PM-4	Plan of Action and Milestones Process	x				x	x		x		x	x
PM-5	System Inventory					x	x				-	x
PM-5(1)	INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION	x				x						x
PM-7	Enterprise Architecture	x				x	x				-	x
PM-9	Risk Management Strategy	x				x	x		x		x	x
PM-10	Authorization Process	x				x	x				x	
PM-11	Mission and Business Process Definition	x					x		x		x	
PM-14	Testing, Training, and Monitoring	x				x	x		x		x	x
PM-18	Privacy Program Plan	x				x					-	
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	x									-	x
PM-30	Supply Chain Risk Management Strategy										x	
PM-30(1)	SUPPLIERS OF CRITICAL OR MISSION-ESSENTIAL ITEMS											

The following controls were not selected to be included in the standard

CONTROL	CONTROL NAME	PRIVACY	SECURITY CONTROL			IRS Publication	MARS-E	CJIS 6.0	HIPAA Security	FERPA	ISO	PCI-DSS
NUMBER	CONTROL ENHANCEMENT NAME	CONTROL	LOW	MOD	HIGH	1075	2.2		Rule 45 C.F.R		270001	v4.0.1
		BASELINE										
PM-2	Information Security Program Leadership Role					x	x				x	x
PM-6	Measures of Performance	x					x		x		x	x
PM-7(1)	OFFLOADING											
PM-8	Critical Infrastructure Plan	x					x		x	x	-	x
PM-13	Security and Privacy Workforce	x					x		x		x	x
PM-15	Security and Privacy Groups and Associations						x		x		x	x
PM-16	Threat Awareness Program						x		x		-	x
PM-16(1)	AUTOMATED MEANS FOR SHARING THREAT INTELLIGENCE											x
PM-17	Protecting Controlled Unclassified Information on External Systems	x									-	
PM-19	Privacy Program Leadership Role	x				x					-	
PM-20	Dissemination of Privacy Program Information	x									-	
PM-20(1)	PRIVACY POLICIES ON WEBSITES, APPLICATIONS, AND DIGITAL SERVICES	x										
PM-21	Accounting of Disclosures	x				x					-	
PM-22	Personally Identifiable Information Quality Management	x									-	
PM-23	Data Governance Body										-	x
PM-24	Data Integrity Board	x									-	x
PM-26	Complaint Management	x									-	
PM-27	Privacy Reporting	x									-	
PM-28	Risk Framing	x									x	x
PM-29	Risk Management Program Leadership Roles					x					x	x
PM-31	Continuous Monitoring Strategy	x									x	x
PM-32	Purposing										-	

Document History/Owner

This standard was developed as required by the State of Wisconsin Information Technology Security Policy Handbook, under the authority of Wis. Stat. § 16.971.

This standard is effective upon approval and publication until retired. Revisions and updates continue the effective date by documenting required changes over time.

Ownership for this standard is assigned to DOA, DET Bureau of Security. As such, the DOA, DET Bureau of Security is responsible for the maintenance, update(s), and review of this document annually before the anniversary of the effective date.

Version #	Revision or Review Date	Description of Change(s)	Reviewer/Author	Date Approved
1.0	6/19/2025	Reviewed with Agency Security Officers, IT Directors and Administrative Officers. Changes were incorporated	Reviewer: WI ISAC, Enterprise IT and AOC Author: DOA/DET/BOS	7/29/2025
NOTE: Keep only the origination and the last 10 years of update information. Only notate prior three revisions. Include only interim/final revision statuses.				

Authorized and approved by:
William Brinkley, State of Wisconsin Chief Information Security Officer

Bill Brinkley	Signed by: William Brinkley BD38B4C11B0F4BB...	7/29/2025 | 9:19 AM CDT
Print/Type Title	Signature	Date