250 – System and Communications 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.

Standard

Based on NIST SP 800-53 Rev. 5, DET's Standards address a diverse set of security and privacy requirements. As a currently established baseline for implementation, DOA utilizes all low level, and selected moderate level controls in support of its security posture initiatives. Agencies shall categorize their data and identify the potential impact (high, moderate, or low), and select controls appropriately as defined by Table 3-1 in NIST SP 800-53B for the allocated impact levels (high, moderate, low) of controls and control enhancements. Agencies shall update DET on the status of their baseline control implementation through the reporting and monitoring process.

Executive Branch Agencies shall develop policies, procedures, or processes for their own State information systems and system environments to protect State information, if applicable. **Note:** Some agencies have specific regulatory requirements to follow that go above and beyond the requirements for other agencies. Implementation of the standard controls within this document 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.

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.

Definitions

Active content - refers to electronic documents/code that can carry out or trigger actions automatically without an individual directly or knowingly invoking the actions. This does not include scheduled batch jobs.

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 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 the agency.

Mobile code technology – Examples include Java, JavaScript, ActiveX Postscript, PDF, Shockwave movies, Flash animations and VBScript.

Exception Process

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

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
2.0	11/03/20	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC/ITDC Author: DOA/DET/BOS	11/11/20
3.0	06/24/22	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC/ITDC Author: DOA/DET/BOS	06/24/22
4.0	7/14/23	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC and Enterprise IT Author: DOA/DET/BOS	08/01/23
5.0	7/2/24	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC and Enterprise IT Author: DOA/DET/BOS	7/30/24
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:

Troy Stairwalt, State of Wisconsin Chief Information Security Officer

DocuSigned by:
Troy Stairwalt
1gFE6C0dFC2524A8...

7/31/2024 | 4:05 PM CDT

Print/Type
Title

Signature

Date