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.

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 (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.

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 that is created, accessed, used, stored, or transmitted by an Executive Branch Agency.

DET/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.

Exception Process

Exceptions to any Executive Branch Agency's Security Policies, Procedures 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	07/14/23	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
524A8...

7/31/2024 | 4:05 PM CDT

Print/Type
Title

Signature

Date