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.

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 (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.

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.

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.

Information Asset – All State information and State information systems and environments.

Exception Process

Exceptions to any Executive Branch Agency's Security Policies 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	Reviewer: WI ISAC/ITDC Author: DOA/DET/BOS	11/11/20

		changes were incorporated		
3.0	06/24/22	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC/ITDC Author: DOA/DET/BO	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/BO	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/BO	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
[illegible]2524A8...

7/31/2024 | 4:05 PM CDT

Print/Type Signature Date
Title