240 - System and Services Acquisition Standard

Purpose

The System (assets) and Services Acquisition standard provides documentation of the minimum requirements for IT Security considerations before, during, and after the IT procurement process to achieve compliance with the System and Services Acquisition Policy.

Standard

This standard uses the NIST SP 800-53 Rev. 5 framework as the guideline to establish control objectives to address a diverse set of security and privacy requirements. Not all controls within NIST SP 800-53 Rev. 5 may be selected for the Statewide baseline policies and standards. Agencies must categorize their data and identify the potential impact (high, moderate, or low), and select controls appropriately. This standard uses Table 3-1 in NIST SP 800-53B for the allocated impact levels (high, moderate, low) of controls and control enhancements. At a minimum, all low controls are selected, and certain moderate controls are selected. Agencies are to reflect their controls through the annual reporting process to DOA-DET.

Executive Branch Agencies are to develop policies, procedures, or processes for their own State information systems and system environments to protect State information, if applicable. 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. Agencies should consider the following for inclusion in their policies, procedures, or processes:

Allocation of Resources (SA-2):

- Determining the high-level information security and privacy requirements for the system or system service in mission and business process planning.
- Allocate resources and funding for information security to be included in assets/services.
- Executive Branch Agencies are required to follow Statewide IT planning, Annual Strategic IT Planning and Million-dollar IT Project Reporting. See the following website for additional documentation: https://detcc.wi.gov/Pages/AgencyReporting.aspx.

System Development Life Cycle (SA-3):

- Acquiring, developing, and managing the system using a system development life cycle process that incorporates information security and privacy considerations.

- Defining and documenting information security and privacy roles and responsibilities throughout the system development life-cycle.
- Identifying individuals having security and privacy roles and responsibilities.
- Integrating Agency information security and privacy risk management process into the system development life cycle activities.

Acquisition Process (SA-4):

- The following security areas must be included/considered prior to the acquisition of any critical infrastructure assets or 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.

System Documentation (SA-5):

- Obtaining or developing administrator documentation for the system, system components, or system services that describes:
  - Security 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.
- Obtaining or developing 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 enables 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.
- Distributing documentation to the appropriate Agency personnel or roles.

Security and Privacy Engineering Principles (SA-8):

- Applying system security engineering principles in the specification, design, development, implementation, and modification of the information system.

External System Services (SA-9):

- Requiring providers of external system services comply with Agency security and privacy requirements.
- Defining and documenting Agency oversite and user roles and responsibilities with regard to external system services.
- Employing processes, methods, and techniques to monitor control compliancy by external service providers on an ongoing basis.

Developer Configuration Management (SA-10):

- Require developers of the systems, system components, or system service to:
  - Perform configuration management during system, component, or services design, development, implementation, operation, and 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 flows and flow resolutions 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 information service to:
  - Develop and implement a plan for ongoing security and privacy assessments.
  - Perform testing and evaluations.
  - Produce evidence of the execution of the security assessment plan and the results for the security testing and evaluation.
  - Implement variable flaw remediation process.
  - Correct flaws identified during security testing and evaluation.

Unsupported System Components (SA-22)

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

Definitions

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

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 Agencies Security Policies, Procedures or Standards must follow the Executive Branch Agencies 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 Wisconsin State Statute 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	10/15/18	Submitted to and approved by the IT Executive Steering Committee	Reviewer: ITESC Author: DOA/DET	10/15/18
1.0	10/29/19	Reviewed with Agency Security Officers and feedback collected. Planning for making revisions.	Bureau of Security	10/29/19
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/BO	06/24/22
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:

Alan Greenberg, CISO

DocuSigned by:
Alan Greenberg
7062227F849B429...

7/8/2022 | 1:55 PM CDT

Print/Type
Title

Signature

Date