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.

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.

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

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 Agencies.

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 (AC-2): Individual, privilege (administrative and default privileged), shared, service, emergency, and temporary accounts.

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 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
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: ITESC Author: DOA/DET	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	07/31/23
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
[illegible]2524A8...

7/31/2024 | 4:05 PM CDT

Print/Type Signature Date
Title