State of Maryland

STANDARD

CONFIGURATION MANAGEMENT

Document No.	Last Updated	Prepared By
MD-STD-305-CM-01	02/18/2026	DOIT OSM

Configuration management is an important aspect of cybersecurity as it helps systems remain in a secure, controlled state, reducing vulnerabilities and minimizing risks complementing a Zero Trust Architecture (ZTA).

PURPOSE AND SCOPE

Purpose	This standard provides the technical and operational specifications needed to manage and maintain system configurations across the State's hardware, software, and network environments.
Scope	This standard provides an organizational approach for maintaining consistency in a State system's functional and physical attributes throughout its lifecycle.
Applicability	This standard applies to all units of State government (as defined in SF&P 3.5-101(g)), hereafter referred to simply as "agencies."
Related Policy	This standard is part of a broader policy suite. Refer to MD-POL-100 Cybersecurity & Governance Policy, Appendix C for a list of related policies and standards.
Baseline	This standard has been developed using National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 Moderate Baseline[1] and State-specific organizationally defined parameters. Agencies may be required to deviate from this baseline when State statute, executive orders, or applicable regulations establish a conflicting requirement that precludes compliance.
Distribution	This document is approved for public distribution and may be shared with external stakeholders, partners, and regulatory bodies. It reflects the State's commitment to transparency, compliance, and operational excellence. Unauthorized modifications or misrepresentation of this document are strictly prohibited.

[1] NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.

FOREWORD

Agencies that use Department of Information Technology DoIT-managed services automatically receive, or *inherit*, the compliance those services already meet, reducing duplicative work and accelerating their overall compliance efforts. These centrally governed services, such as hosting platforms, identity management, and network infrastructure, are built with robust control frameworks that automatically extend to participating agencies. By leveraging these offerings, agencies not only align with key operational and security standards but also benefit from pre-configured environments, continuous monitoring, and policy enforcement mechanisms maintained by DoIT. Agencies are encouraged to leverage these services to accelerate readiness, gain cost efficiency, simplify compliance efforts, and allow agencies to focus more fully on mission delivery, knowing that foundational requirements are already in place. Agencies should review the scope of each managed service to understand which standards are inherited and where additional agency-specific controls may still be required.

GUIDANCE AND ENFORCEABILITY

Throughout this document, informational call-out boxes are utilized to provide additional context or elaborate on key topics. While these boxes primarily serve an informational purpose, any directives or mandated actions contained within them are authoritative and carry the same enforceability as the core requirements of this document. For the purposes of this document, the term “shall” denotes a mandatory requirement. Terms such as “where feasible”, “encouraged”, or similar phrasing indicate recommended practices that reflect organizational preference but are not enforceable requirements at this time.

CHANGE RECORD

Version	Summary of Changes	Changed By	Date
1.0	Initial Publication	Miheer Khona	02/18/2026

STANDARDS

305 State Strategy

These standards establish a baseline of configuration management practices that each agency must implement to comply with State cybersecurity and privacy policies. Each agency shall designate specific personnel with IT responsibilities to ensure the effective implementation of these standards.

305-1 Develop Agency-Level Procedures (CM-1)

In alignment with this standard, develop and document agency-level configuration management procedures. Agencies must disseminate the procedures to agency personnel with information technology (IT) security responsibilities. Agencies must review, and if needed, update the procedures as deemed appropriate by the agency based on changes and risk at least every 3 years. At a minimum, the procedures must address purpose, scope, roles and responsibilities, and guidelines.

305-2 Establish Baseline Configurations (CM-2)

Develop and maintain version-controlled, agency-defined baseline configurations for each system, including hardware, software, firmware, and security. Review and update the baseline configuration at least **annually** and when significant changes occur, including the installation or upgrade of system components. Type of changes include but are not limited to:

- Configuration changes;
- Configuration items;
- Patches/updates;
- Security-relevant settings; and
- Operational/procedural changes.

Zero Trust Architecture

As the State moves toward ZTA and continuous verification of devices accessing the network, documented baselines should include, at a minimum: a) Versions of compilers used; b) Build options when creating applications/components; c) Versions of commercial off-the-self (COTS) Software used as part of an application; d) Software bill of materials (SBOM); e) For web applications, which browsers and what versions are supported; f) All known security assumptions, implications, system level protections, best practices, and required permissions in alignment with industry best practices and vendor recommendations; and g) Deployment configuration settings (e.g., encryption settings (data in transit), public key infrastructure (PKI) certificate configuration settings, and password settings).

CM-2(2): Maintain the currency, completeness, accuracy, and availability of the baseline configuration of each system using automated mechanisms where feasible for continuous verification of devices accessing the network, consistent with ZTA principles.

Continuous Device Verification Tools

Examples of automated mechanisms include: a) Endpoint Detection and Response (EDR) tools; b) Mobile Device Management (MDM)/Unified Endpoint Management (UEM) platforms; c) Network Access Control (NAC) solutions; d) Continuous authentication via Artificial Intelligence/Machine Learning; e) Security Information and Event Management (SIEM) solutions; f) Security Orchestration, Automation, and Response (SOAR) tools; g) Certificate-based authentication mechanisms; and h) Cloud Access Security Brokers (CASB).

CM-2(3): Retain at least a single iteration of previous versions of baseline configurations of the system (e.g., hardware, software, firmware, configuration files) to support rollback.

CM-2(7): Coordinate with DoIT to obtain or approve the appropriately configured IT assets for individuals traveling to locations outside the U.S. and its Territories; and implement the DoIT-defined procedures when the individuals return from travel.

305-3 Maintain Configuration Change Control (CM-3)

Identify and document which system changes are subject to configuration control. Review the configuration-controlled changes prior to implementation by performing a security/privacy impact analysis. Implement configuration-controlled changes to the system only as approved; Retain records of configuration-controlled changes to the system in accordance with applicable records retention schedule and applicable legal/regulatory requirements, and ensure they remain available for audit and incident investigations for the life of the system; Monitor configuration change control activities continuously (e.g., ticketing, audit logs, metrics) and conduct reviews **quarterly**, or more frequently for High Value State System (HVSS); and Coordinate and provide oversight for configuration change control activities through a Configuration Control Board (CCB), or equivalent change authority, that convenes regularly to review upcoming configuration changes.

CM-3(2): Test, validate, and document changes to the system before finalizing the implementation of the changes.

CM-3(4): Require designated agency security and privacy representatives to be members of the CCB.

Continuous Integration/Continuous Delivery-Driven Change Control

To promote automation, agencies should create a strategy to implement automation and Continuous Integration (CI) and Continuous Delivery (CD) methodologies within the Change Control process. This approach uses a dynamic, policy-driven, and tool-integrated workflow, not a static approval gate. Tools like ServiceNow DevOps, Jira, or Azure DevOps can be integrated to auto-generate and track change records.

305-4 Perform Impact Analyses (CM-4)

Except for changes that are driven by security updates or maintenance (i.e. operating system (OS) patching, browser updates), and prior to change implementation, analyze changes, to system components performing a security function to determine potential security and privacy impacts.

CM-4(2): After system changes, verify that the impacted security and privacy controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

305-5 Implement Access Restrictions for Change (CM-5)

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system. Implement a formal approval process for granting individuals the authority to perform system changes.

305-6 Document Configuration Settings (CM-6)

Establish, document, and implement configuration settings for components employed within each system that reflect the most restrictive mode consistent with operational requirements using DoIT standards and industry best practices (e.g., Center for Internet Security (CIS) Benchmarks, vendor recommendations).

Identify, document, and approve deviations from established configuration settings for system components (e.g., servers, workstations, network devices, databases). Deviations shall be documented in the System Security Plan (SSP) or other approved configuration management artifacts, including justification and risk acceptance where applicable. Monitor and control configuration changes in accordance with the organization’s configuration management and change control processes.

305-7 Implement Least Functionality (CM-7)

Configure the system to provide only essential capabilities.

CM-7(1): Review system settings at least **quarterly** to identify, disable and remove unnecessary functions, ports, protocols, software, and services that are not required for system operation or that deviate from approved secure configuration benchmarks (e.g., CIS Benchmarks, vendor security recommendations).

CM-7(2): Only approved software may run on information systems, as defined by the authorized software list and CCB approvals.

CM-7(5): Maintain an agency-approved software list for each system, enforce a deny-all/ permit-by-exception execution policy, and review and update the authorized software list **annually**.

Baseline Scanning

System configuration baselines represent the secure, approved state of a device, covering things like OS settings and access control settings. Scanning for baseline compliance ensures that systems haven't drifted from these hardened configurations, which can happen due to manual changes, software updates, or misconfigurations. Unlike patch scans, baseline checks reveal hidden risks that aren't tied to missing updates but can still expose systems to exploitation or non-compliance.

305-8 Maintain System Component Inventory (CM-8)

Develop and document an inventory of agency systems and system components that: a) Accurately reflects each system; b) Includes all components within the authorization boundary; c) Does not include duplicate accounting of components or components assigned to more than one system; and d) Is at the level of granularity deemed necessary for tracking and reporting. Review and update the system component inventory at least **annually** or when changes occur.

At a minimum, hardware inventory shall include:

- Component accountability;
- Inventory requirements;
- Hardware Media Access Control (MAC) address;
- Point of contact or owner;
- Instance tag or serial number;
- OS name, version number, and patch level;
- Fully Qualified Domain Name (FQDN);
- Internet Protocol (IP) address/hostname;
- Make and model; and
- Physical Location.

At a minimum, software inventory shall include:

- Point of contact;
- License type;
- Software name;
- Version; and
- SBOM.

CM-8(1): Update the inventory of system components as part of component installations, removals, and system updates.

CM-8(3): Detect the presence of unauthorized hardware, software, and firmware components within each system using automated mechanisms for real-time detection where possible (at least **weekly** if not automated); and when unauthorized components are detected, disable network access and notify the system owner, agency official, State Security Operations Center (SOC), and State Chief Information Security Officer (SCISO).

305-9 Develop a Configuration Management Plan (CM-9)

Develop, document, and implement a configuration management plan for each system that: a) Addresses roles, responsibilities, and configuration management processes and procedures; b) Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c) Defines the configuration items for each system and places the configuration items under configuration management; d) Is reviewed and approved by the appropriate agency Authorizing Official; and e) Protects the configuration management plan from unauthorized disclosure and modification.

305-10 Enforce Software Usage Restrictions (CM-10)

Use software and associated documentation in accordance with contract agreements and copyright laws; Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and Control and document the use of peer-to-peer file sharing technology to prevent this capability from being used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

305-11 Restrict User-installed Software (CM-11)

Establish agency procedures governing the installation of software by users. Enforce software installation rules through automated methods (where possible). Monitor procedure compliance **semiannually**.

305-12 Monitor Information Location (CM-12)

Identify and document the location of State data 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.

CM-12(1): Consistent with guidance from the Agency Data Officer (ADO), or State Chief Data Officer (SCDO) where there is no ADO, use automated tools to identify agency information by type and the system components that store/process the information to adequately implement security controls to protect State data.

GUIDELINES

ID	Title	Description	Source
CSF Tools	Cybersecurity Framework Tools	This website provides supplemental guidance for each security control listed in this document.	*csf.tools (LINK)*
NIST SP 800-128	Guide for Security-Focused Configuration Management of Information Systems	This document provides guidelines for managing and administering the security of Federal information systems, emphasizing security-focused configuration management (SecCM).	*csrc.nist.gov (LINK)*

DEFINITIONS

Each unique term used in this standard is defined in the **State of Maryland Cybersecurity & Privacy Glossary**.

COMPLIANCE CHECKLIST

ID	Standard	Compliance
305-1	**Develop Agency-Level Procedures (CM-1)**	☐ Yes ☐ No
305-2	**Establish Baseline Configurations (CM-2)**	☐ Yes ☐ No
305-3	**Maintain Configuration Change Control (CM-3)**	☐ Yes ☐ No
305-4	**Perform Impact Analyses (CM-4)**	☐ Yes ☐ No
305-5	**Implement Access Restrictions for Change (CM-5)**	☐ Yes ☐ No
305-6	**Document Configuration Settings (CM-6)**	☐ Yes ☐ No
305-7	**Implement Least Functionality (CM-7)**	☐ Yes ☐ No
305-8	**Maintain System Component Inventory (CM-8)**	☐ Yes ☐ No
305-9	**Develop a Configuration Management Plan (CM-9)**	☐ Yes ☐ No
305-10	**Enforce Software Usage Restrictions (CM-10)**	☐ Yes ☐ No
305-11	**Restrict User-installed Software (CM-11)**	☐ Yes ☐ No
305-12	**Monitor Information Location (CM-12)**	☐ Yes ☐ No

Note: When assessing the implementation and effectiveness of the security and privacy controls outlined in this standard, DoIT recommends the use of NIST SP 800-53A Rev. 5, to perform evaluations in a manner that is evidence-based, repeatable, and aligned with the system's documented security posture.