State of Maryland

STANDARD

MAINTENANCE

Document No.	Last Updated	Prepared By
MD-STD-309-MA-01	02/18/2026	DOIT OSM

A maintenance standard establishes consistent procedures for monitoring, updating, and servicing technology systems to ensure reliability, security, and performance. By formalizing these practices, organizations reduce downtime, prevent vulnerabilities, and support long-term operational resilience.

PURPOSE AND SCOPE

Purpose	This standard provides the technical and operational specifications needed to maintain effective security controls over time.
Scope	This standard addresses security-focused maintenance and supply chain considerations.
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.
Distributions	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

309 State Strategy

These standards establish a baseline of maintenance 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.

309-1 Develop Agency-Level Procedures (MA-1)

In alignment with this standard, develop and document agency-level maintenance 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.

309-2 Conduct Controlled Maintenance (MA-2)

Control maintenance activities as follows:

- Plan and communicate maintenance windows at least **monthly** for all systems and services to accommodate maintenance updates (e.g., upgrades, configuration changes, and patching);
- Require authentication and authorization in accordance with State cybersecurity and privacy standards for all maintenance personnel, ensuring least privilege access;
- Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
- Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;
- Require that the system owner explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;
- Sanitize equipment to remove State data from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement;
- Check all potentially impacted security and privacy controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and

- Include the following information in organizational maintenance records: a) Date & time of maintenance; b) Name of individual or group performing maintenance; c) Description of maintenance performed; d) Information system components removed or replaced during the maintenance; e) Software components removed or replaced; and f) Name of escort (if necessary).

309-3 Use Approved Maintenance Tools (MA-3)

Approve, control, and monitor the use of system maintenance tools. Enforce endpoint security policies and monitor tool usage to detect anomalies. Review previously approved system maintenance tools at least **annually**.

MA-3(1): Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

Verifying Tool Integrity
To verify tool integrity, consider the following: a) Checksum or hash validation, comparing against known-good values; b) Digital signatures to confirm authenticity from trusted vendors; c) Source verification, ensuring tools are downloaded from official, secure sources; d) Check for physical tampering; e) Scan for unauthorized code, embedded scripts, or unexpected behavior; and f) Use endpoint protection or sandboxing to test tools in a controlled environment.

MA-3(2): Check media containing diagnostic and test programs for malicious code before the media are used in the system.

MA-3(3): Prevent the removal of maintenance equipment containing organizational information by: a) Verifying that there is no organizational information contained on the equipment; b) Sanitizing or destroying the equipment; c) Retaining the equipment within the facility; or d) Obtaining approval from the apprporiate Authorizing Official for removal of the equipment from the facility.

309-4 Monitor Non-local Maintenance (MA-4)

Obtain prior authorization and monitor non-local maintenance and diagnostic activities; Allow the use of non-local maintenance and diagnostic tools only when using an authorized secure remote capability (i.e. Secure Access Service Edge (SASE)) and enforcing multi-factor authentication (MFA) and continuous monitoring as documented in the System Security Plan (SSP). Maintain records for non-local maintenance and diagnostic activities. Terminate sessions and network connections when non-local maintenance is completed.

309-5 Authorize Maintenance Personnel (MA-5)

Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel. Verify that unescorted personnel performing maintenance on the system possess the required access authorizations. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

309-6 Perform Timely Maintenance (MA-6)

Obtain maintenance support and/or spare parts for agency systems within **48 hours** of failure or as otherwise defined in maintenance agreements and the system contingency plan.

GUIDELINES

ID	Title	Description	Source
CSF Tools	Cyber Security Framework Tools	This website provides supplemental guidance for each security control listed in this document.	*csf.tools (LINK)*

DEFINITIONS

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

COMPLIANCE CHECKLIST

ID	Standard	Compliance
309-1	**Develop Agency-Level Procedures (MA-1)**	☐ Yes ☐ No
309-2	**Conduct Controlled Maintenance (MA-2)**	☐ Yes ☐ No
309-3	**Use Approved Maintenance Tools (MA-3)**	☐ Yes ☐ No
309-4	**Monitor Non-local Maintenance (MA-4)**	☐ Yes ☐ No
309-5	**Authorize Maintenance Personnel (MA-5)**	☐ Yes ☐ No
309-6	**Perform Timely Maintenance (MA-6)**	☐ 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.