State of Maryland

STANDARD

SYSTEM & INFORMATION INTEGRITY

Document No.	Last Updated	Prepared By
MD-STD-319-SI-01	02/18/2026	DOIT OSM

System and Information Integrity are crucial for maintaining the reliability, security, and trustworthiness of an organization's information technology (IT) infrastructure through real-time monitoring, automated threat detection, and strict access controls. Within a Zero Trust Architecture (ZTA), integrity controls play a vital role in continuously verifying the security posture of systems and data, ensuring that no entity, whether internal or external, is inherently trusted.

PURPOSE AND SCOPE

Purpose	This standard provides the technical and operational specifications needed for data to remain accurate, unaltered, and protected from unauthorized modifications.
Scope	This standard addresses controls that help detect and respond to unauthorized changes, protect against malicious code, and maintain data accuracy and reliability.
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

319 State Strategy

These standards establish a baseline of system and information integrity protections and 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.

319-1 Develop Agency-Level Procedures (SI-1)

In alignment with this standard, develop and document agency-level system and information integrity procedures. Agencies must disseminate the procedures to agency personnel with 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 that enforce ZTA principles.

319-2 Perform Flaw Remediation (SI-2)

Identify, report, and correct system flaws better known as vulnerabilities. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation. Install security-relevant software and firmware updates within the timeline defined below, based on vulnerability severity level and the date of update release. Incorporate flaw remediation into the agency configuration management process.

Severity Levels & Remediation Timeline

Severity Level	CVSS Score Range*	Remediation Timeline
Critical	9.0 - 10.0	Within 15 calendar days
High	7.0 – 8.9	Within 30 calendar days
Moderate	4.0 – 6.9	Within 60 calendar days
Low	0.1 – 3.9	Within 90 calendar days

** NIST National Vulnerability Database (NVD)*

Installation timelines for security-relevant software and firmware updates may vary according to platform-specific patching schedules. Critical updates, including those listed in the CISA Known Exploited Vulnerabilities (KEV) catalog, may be deployed on an expedited basis at the discretion of the State Chief Information Security Officer (SCISO) or when required by KEV deadlines. Agencies unable to meet emergency timelines due to essential business operations must immediately notify DoIT OSM and apply compensating controls, such as network isolation, heightened monitoring, or temporary service suspension, until patching is completed.

CISA Known Exploited Vulnerabilities

CISA maintains an authoritative list of software vulnerabilities that are confirmed to be actively exploited in the wild. This catalog is maintained to help organizations prioritize patching by focusing on vulnerabilities that attackers are actually exploiting, rather than just those theoretically possible. Includes vulnerabilities across vendors, products, and platforms that have been observed in real-world attacks. State agencies are required to remediate KEVs by the specific deadlines defined by CISA which may be sooner than 15 days, depending on the severity, exploitation status, and risk profile of the vulnerability.

SI-2(2): Determine if system components have applicable security-relevant software and firmware updates installed using continuous monitoring tools such as vulnerability scanners and patch management platforms.

319-3 Implement Malicious Code Protection (SI-3)

Implement modern threat detection technologies (e.g., Signature based, heuristic analysis, and artificial intelligence (AI)-enabled detection) for malicious code protection at system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices) to detect and eradicate malicious code. Automatically update malicious code protection mechanisms as new releases are available in accordance with agency configuration management policy and procedures.

Configure malicious code protection mechanisms to:

- Perform periodic scans of the system regularly and real-time scans of files from external sources at endpoints and network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational policy;
- Implement cloud workload protection platforms, cloud security posture management capabilities, AI/Machine Learning (ML)-based threat detection, and sandboxing for dynamic analysis of the cloud environment;
- Block or quarantine malicious code and send alert to a system administrator and MD-Security Operations Center (SOC) in response to malicious code detection; and
- Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

Endpoint Detection and Response Integration for Proactive Malware Prevention

To strengthen cybersecurity posture across enterprise environments, State agencies are to collaborate with the DoIT Office of Security Management (OSM) to implement endpoint detection and response (EDR) solutions that incorporate real-time behavioral analytics. Where feasible, this integration should be pursued at the enterprise level to enhance threat visibility and proactively prevent malware execution. By leveraging EDR technologies that analyze endpoint activity in real time, agencies can detect anomalous behavior indicative of malicious intent, enabling faster incident response and reducing the risk of compromise. This collaborative approach supports a unified security framework, aligns with best practices in threat prevention, and reinforces the resilience of public sector IT infrastructure.

319-4 Perform System Monitoring (SI-4)

Monitor the system to detect:

- Attacks and indicators of potential attacks;
- Unauthorized local, network, and remote connections;
- Identify unauthorized use of the system through intrusion detection/prevention systems (IDS/IPS), malicious code protection software, scanning tools, and audit records monitoring;
- File Integrity monitoring;
- Application Programming Interface (API) security monitoring and rate limiting;
- Privileged access monitoring with session recording;
- Data loss prevention (DLP) monitoring; and
- Cloud infrastructure monitoring to include configuration drift detection.

Invoke internal monitoring capabilities and deploy monitoring devices:

- Strategically within the system to collect information determined by the agency as essential; and
- At ad hoc locations within the system track specific types of transactions of interest to the agency or DoIT.

Agencies shall analyze detected events and anomalies and adjust system monitoring activities when changes in risk to agency operations, assets, individuals, or the State are identified. Monitoring information indicating suspected or confirmed security incidents, unauthorized activity, or other high-risk attack indicators shall be reported to the MD SOC within **1 hour** of discovery. Routine alerts that do not indicate elevated risk may be handled through standard operational monitoring processes. Agencies shall obtain legal review of system monitoring activities as appropriate.

SI-4(2): Automated tools must be employed for near real-time analysis of events (i.e., within seconds to minutes of occurrence and not human driven) supporting a dynamic risk posture that enables agencies to respond to threats as they emerge, rather than on fixed review cycles.

Perform continuous monitoring, leveraging OSM Security Information and Event Management (SIEM) and User Behavior Analytics (UBA) to the extent feasible.

SI-4(4): Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic; Monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.

SI-4(5): Alert MD-SOC within **1 hour** of receipt of system-generated indications of compromise that are considered high-risk (i.e., correlated authentication anomalies indicating suspected compromise); Routine authentication failures are not subject to the one-hour reporting requirement. Indicators requiring notice include, but are not limited to:

- Suspicious security policy changes;
- Suspicious account changes;
- Audit Logs cleared;
- Unauthorized packets based on suspected attack;
- Attempt to bypass system security mechanisms;
- Access to selected privileged files and applications; and
- Any other activities inconsistent with typical pattern of use.

Alerts must be written to local and remote consoles, and the administrator must acknowledge the alert. The alert and acknowledgement should be logged. Administrator acknowledgement is an internal logging requirement and does not delay or extend the **1 hour** SOC notification timeline.

319-5 Implement Security Alerts, Advisories, and Directives (SI-5)

Establish a channel for receipt of system security alerts from vendors and the MD-Information Sharing and Analysis Center (ISAC) on an ongoing basis. Collaborate with DoIT OSM regarding the need to generate internal security alerts, advisories, and directives (if necessary).

Disseminate security alerts, advisories, and directives to: a) Agency personnel with IT and cybersecurity roles; b) Internal stakeholders impacted by the alerts; and c) DoIT OSM if external service providers or mission/business partners are impacted.

Implement State security directives (i.e., Emergency Directives, Binding Operational Directives) in accordance with established time frames and notify DOIT OSM regarding organization non-compliance.

Adaptive Threat Response

To enhance enterprise resilience and align with ZTA principles, agencies should, where feasible, implement adaptive security responses that react dynamically to evolving threat intelligence. This approach enables systems to automatically adjust access controls, isolate compromised assets, and reconfigure defenses based on real-time insights. By integrating adaptive mechanisms into the broader ZTA framework, organizations can reduce dwell time, limit lateral movement, and respond to emerging threats with greater precision.

319-6 Maintain Software, Firmware, and Information Integrity (SI-7)

Employ integrity verification tools to detect and respond to unauthorized changes to software, firmware, and information.

SI-7(1): Perform an integrity check of software, firmware, and information **monthly** for High Value State Systems (HVSS) and any system deemed high criticality, and at least **quarterly** for moderate to low criticality systems. Monitoring examples include, but are not limited to:

Integrity Monitoring

Target	Examples
System Files & Executables	Operating system binaries and registry entries.
File System Changes	File changes, permission changes, hidden files.
Security and Access Controls	Privilege escalations, access control lists (ACLs), user or group accounts.
System State & Behavior	Running processes/services, scheduled tasks, boot records and start up scripts.
Network & Communications	Firewall rules and routing tables, Domain Name Systems (DNS) configurations, network interface settings.
Logs & Audit Trails	System, security, and application logs; rotation and archival settings.
Application Integrity	Web server configurations, database schemas, API keys and secrets.
Cryptographic Elements	Certificates and keys, hashes and checksums, secure boot configurations.

SI-7(7): Incorporate the detection of unauthorized changes to established configuration settings and unauthorized elevation of information system privileges into the organizational incident response capability. Where feasible, implement cryptographic integrity verification and secure boot mechanisms to prevent unauthorized modifications.

319-7 Implement Spam Protection (SI-8)

Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Centralized Spam and Phishing Protection

Agencies are strongly encouraged to leverage the enterprise-provided spam and phishing protection solution as their sole mechanism for securing email traffic, rather than procuring or deploying independent tools, to ensure consistent threat intelligence, centralized monitoring, and uniform compliance across the State.

SI-8(2): Automatically update spam protection mechanisms when new releases are available.

319-8 Perform Information Input Validation (SI-10)

Check the validity of any information input where syntax can be validated, and ensure inputs match specified definitions or are rejected.

319-9 Perform Error Handling (SI-11)

Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited. Reveal error messages only to authorized personnel such as system administrators.

Detailed error outputs, and error outputs that include non-public data, must be adequately protected. For applications, agencies should also verify that applications are secure during startup and shutdown, as well as conduct application security testing prior to application releases.

Application Security Testing

Application security testing techniques, designed to identify vulnerabilities, misconfigurations, and weaknesses in applications before they can be exploited, include but are not limited to: a) Static Application Security Testing (SAST) that analyzes source code, bytecode, or binaries without executing the program, helping developers catch issues early in the development lifecycle; b) Dynamic Application Security Testing (DAST), which evaluates running applications to identify vulnerabilities in real-time, simulating external attacks without access to the underlying code; c) Interactive Application Security Testing (IAST) combines elements of both SAST and DAST, offering real-time feedback by monitoring applications from within during runtime; and d) Software Composition Analysis (SCA) which focuses on identifying known vulnerabilities in third-party libraries and open-source components. Penetration testing may also be used to simulate real-world attacks to uncover exploitable flaws.

319-10 Manage and Retain Information (SI-12)

Manage and retain information and output in accordance with all applicable laws, executive orders, directives, regulations, and operational requirements. As per MD-POL-205 Data Protection & Privacy Policy, agencies must define and document retention requirements with the appropriate data custodian(s) using a data retention agreement.

Privacy information requires strict adherence to retention standards approved by the Chief Privacy Officer (SCPO). Additionally, to minimize risk, privacy information must not be used in non-production environments; sample simulated data should be leveraged instead.

319-11 Implement Memory Protection (SI-16)

Implement the following controls to protect the system memory from unauthorized code execution: a) Memory protection on system components using either hardware or software-based data execution prevention; and b) Address space layout randomization to protect its memory from unauthorized code execution.

319-12 De-Identification (SI-19)

Remove the elements of Personally Identifiable Information (PII) from datasets in accordance with Chief Privacy Officer standards; and evaluate **annually** for effectiveness of de-identification.

De-Identification

De-identification is a privacy-enhancing process used to reduce the risk of exposing PII by removing or obscuring data elements that can directly or indirectly identify an individual. De-identification involves techniques such as masking, pseudonymization, aggregation, or suppression to ensure that sensitive attributes (e.g., Names, Social Security numbers (SSNs)) cannot be traced back to a specific person. While de-identified data may still retain analytical value for research or operational purposes, it must be handled carefully to prevent re-identification through data linkage or inference.

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)*
NIST SP 800-215	Guide to a Secure Enterprise Network Landscape	This document provides security guidance for modern enterprise networks, addressing challenges such as cloud access, micro-services-based applications, and geographically distributed IT resources.	*csf.tools (LINK)*
NIST SP 800-88	Guidelines for Media Sanitization	This document provides best practices for securely disposing of data stored on various types of media to prevent unauthorized access or data recovery.	*csf.tools (LINK)*
NIST SP 800-133	Recommendation for Cryptographic Key Generation	This document provides guidance on secure key generation methods for approved cryptographic algorithms.	*csf.tools (LINK)*
NIST SP 800-28	Guidelines on Active Content and Mobile Code	This document provides guidelines on active content and mobile code, focusing on security risks and mitigation strategies.	*csf.tools (LINK)*
CISA Known Exploited Vulnerabilities Catalog	Known Exploited Vulnerabilities Catalog	The authoritative source of vulnerabilities that have been exploited in the wild as an input to vulnerability management prioritization.	*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
319-1	**Develop Agency-Level Procedures (SI-1)**	☐ Yes ☐ No
319-2	**Perform Flaw Remediation (SI-2)**	☐ Yes ☐ No
319-3	**Implement Malicious Code Protection (SI-3)**	☐ Yes ☐ No
319-4	**Perform System Monitoring (SI-4)**	☐ Yes ☐ No
319-5	**Implement Security Alerts, Advisories, and Directives (SI-5)**	☐ Yes ☐ No
319-6	**Maintain Software, Firmware, and Information Integrity (SI-7)**	☐ Yes ☐ No
319-7	**Implement Spam Protection (SI-8)**	☐ Yes ☐ No
319-8	**Perform Information Input Validation (SI-10)**	☐ Yes ☐ No
319-9	**Perform Error Handling (SI-11)**	☐ Yes ☐ No
319-10	**Manage and Retain Information (SI-12)**	☐ Yes ☐ No
319-11	**Implement Memory Protection (SI-16)**	☐ Yes ☐ No
319-12	**De-Identification (SI-19)**	☐ 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.