State of Maryland

STANDARD

SYSTEM AND SERVICES ACQUISITION

Document No.	Last Updated	Prepared By
MD-STD-317-SA-01	02/18/2026	DOIT OSM

System and services acquisition is crucial for ensuring that organizations obtain, integrate, and maintain the right technology solutions, manage third-party relationships, embed security into acquisition processes, and meet organizational and regulatory standards throughout the system lifecycle.

PURPOSE AND SCOPE

Purpose	This standard provides the technical and operational specifications needed to effectively procure, develop, and maintain technology solutions that align with security, operational, and business objectives in a secure manner.
Scope	This standard addresses the activities needed to obtain, develop, and integrate technology solutions securely and efficiently, with a particular focus on procurement processes.
Applicability	This standard applies to all units of State government (as defined in SF&P 3.5-101(g)), hereafter referred to as 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

317 State Strategy

These standards establish a baseline of system and services acquisition 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.

317-1 Develop Agency-Level Procedures (SA-1)

Develop and document agency-level acquisition procedures that incorporate cybersecurity and privacy requirements in system and service acquisition through:

- Alignment with existing Department of General Services Office of State Procurement requirements;
- Alignment with Office of Security Management (OSM) Enterprise standards; and
- Agency supplemental procedures as needed to meet this standard.

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.

317-2 Document and Allocate Resources (SA-2)

Determine the high-level information security and privacy requirements for the system or service being considered for acquisition as part of mission and business process planning. Determine, document, and allocate the resources required to protect the system or service as part of the organizational capital planning and investment control process. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

317-3 Implement System Development Life Cycle (SA-3)

Acquire, develop, and manage the system in alignment with DoIT's Enterprise Architectural Standards using a system development life cycle (SDLC) that incorporates information security and privacy considerations. Define and document information security and privacy roles and responsibilities throughout the SDLC. Identify individuals having information security and privacy roles and responsibilities. Integrate the organizational information security and privacy risk management process into SDLC activities.

317-4 Integrate Cybersecurity into the Acquisition Process (SA-4)

Include the following requirements, descriptions, and criteria, explicitly or by reference, using standardized contract language, reviewed and approved by the State Chief Information Security Officer (SCISO) in the contract for the system, system component, or system service:

- Security and privacy functional requirements;
- Strength of mechanism requirements;
- Security and privacy assurance requirements;
- Controls needed to satisfy the security and privacy requirements;
- Evaluation criteria that assesses the vendor's ability to support Zero Trust Architecture (ZTA), prioritizing solutions with least privilege access, continuous monitoring, and identity-based controls;
- Security and privacy documentation requirements, including requirements for protecting such documentation;
- Description of the system development environment and the intended operational environment;
- Allocation of responsibilities for information security, privacy, and supply chain risk management
- Acceptance criteria.

FedRAMP & GovRAMP Authorization

To ensure the confidentiality, integrity, and availability of State data hosted in cloud environments, the SCISO strongly encourages the use of cloud service offerings (CSO) that have a valid Federal Risk and Authorization Management Program (FedRAMP) or Government Risk and Authorization Management Program (GovRAMP) Authorization. These programs provide independent validation of a cloud service provider's implementation and effectiveness of NIST-based security controls. By choosing FedRAMP/GovRAMP-authorized CSOs, agencies gain audit-ready infrastructure, built-in control mappings, and interoperability across federal and state systems, reducing risk while boosting operational agility. This provides a strong foundation for resilient, compliant modernization.

At a minimum, all service providers must provide at least one of the following: a) FedRAMP or GovRAMP authorization; b) an independent, third-party SOC 2 Type 2 attestation; c) a valid ISO/IEC 27001 certification issued by an accredited certification body; or d) an independent, third-party validation of adherence to another industry-recognized security assurance framework appropriate to the scope of services (e.g., CMMC, PCI DSS, HITRUST, CJIS), as approved by the SCISO. The SCISO may also establish and approve standard contract language specifying when each assurance mechanism is required based on service type, risk level, or procurement category.

For SOC 2 Type 2 to be acceptable the attestation report must demonstrate an unqualified opinion, meaning the auditor found no material exceptions in the controls tested, on the Security Common Criteria (CC) criteria, specifically showing operational effectiveness in Logical Access Controls (CC6), System Operations/Incident Response (CC7), and Risk Assessment (CC3).

SA-4(1): Require the developer of the system, system component, or system service to provide a description of the functional properties of the security and privacy controls to be implemented.

SA-4(2): Require the developer of the system, system component, or system service to provide design and implementation information for the controls that may include, where appropriate: a) Security-relevant external system interfaces; b) High-level security design; and c) Security features configurable by the State.

Shared Responsibility Model

A shared responsibility model defines the division of security obligations between the agency and its external vendors or service providers, particularly cloud and hybrid environments. While the agency retains responsibility for data governance, identity management, and user access, the provider is accountable for securing infrastructure, platform components, and service availability. Each vendor should supply a **Customer Responsibility Matrix (CRM)** that clearly outlines which controls they manage versus those the agency must implement. This transparency is essential for compliance mapping, risk assessments, and ensuring no critical gaps exist in the overall security posture.

SA-4(9): Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for agency use.

317-5 Maintain System Documentation (SA-5)

Obtain or develop a System Security Plan (SSP) for the system, system component, or system service that describes: a) Secure configuration, installation, and operation of the system, component, or service; b) Effective use and maintenance of security and privacy functions and mechanisms; and c) Known vulnerabilities regarding configuration and use of administrative or privileged functions.

Obtain or develop user documentation for the system, system component, or system service that describes:

- User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;
- Methods for user interaction, which enable individuals to use the system, component, or service in a more secure manner and protect individual privacy; and
- User responsibilities in maintaining the security of the system, component, or service and privacy of individuals.

Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and consult the agency CISO (or delegate) to determine if any additional risk mitigations may be required.

317-6 Require Adherence to Security and Privacy Engineering Principles (SA-8)

Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the State.

Zero Trust Architecture

Secure-by-design principles applied to systems, whether developed internally or acquired, builds resilience. Micro-segmentation isolates resources and limits lateral movement, adaptive authentication dynamically verifies user and device trustworthiness, and real-time risk assessments continuously evaluate context and enforce policy decisions.

317-7 Require Secure External System Services (SA-9)

Require that providers of external system services comply with established security and privacy requirements. Define and document organizational oversight and user roles and responsibilities with regard to external system services. Employ agency-authorized processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis.

SA-9(2): Require providers of external system services to identify the functions, ports, protocols, and other services required for the use of such services. Mandate strict access controls and continuous verification for third-party services, to reduce supply chain risks.

317-8 Require Developer Configuration Management (SA-10)

Require the developer of the system, system component, or system service to:

- Perform configuration management during system, component, or service design, development, implementation, operation, and disposal;
- Document, manage, and control the integrity of changes to agency-defined configuration items under configuration management;
- Implement only organization-approved changes to the system, component, or service;
- Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and
- Track security flaws and flaw resolution within the system, component, or service and report findings to the agency CISO (or delegate).

317-9 Require Developer Testing and Evaluation (SA-11)

Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:

- Develop and implement a plan for ongoing security and privacy control assessments;
- Perform functional testing (e.g., unit, integration, system, and/or regression testing) at least **annually**;
- Leverage automated software security testing tools (e.g., static/dynamic application security testing, API security testing, penetration testing) for all systems processing information defined by the state as either confidential (Data Classification Level 3) or restricted (Data Classification Level 4);
- Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;
- Implement a verifiable flaw remediation process; and
- Correct flaws identified during testing and evaluation.

Adaptive Security Testing for System Integration

Before integrating new systems into an operational environment, organizations should, where feasible, conduct rigorous automated security testing that goes beyond traditional vulnerability scans. This includes leveraging behavior analytics to detect anomalous user or system activity and deploying automated threat detection tools that can identify indicators of compromise in real time. By applying these advanced techniques early in the integration process, teams can proactively uncover hidden risks, validate system resilience, and ensure that access controls and response mechanisms are aligned with current threat landscapes and compliance requirements.

Production and non-production environments present distinct risk profiles. To mitigate cross-environmental risk, non-production systems must be both logically and physically segregated from production systems. The use of production data that has not been sanitized in non-production environments is strictly prohibited unless explicitly authorized by the appropriate Authorizing Official.

317-10 Require Development Process, Standards, and Tools (SA-15)

Require the developer of the system, system component, or system service to follow a documented development process that:

- Explicitly addresses security and privacy requirements;
- Identifies the standards and tools used in the development process;
- Documents the specific tool options and configurations used in the development process; and
- Documents, manages, and verifies the integrity of changes to the process and/or tools used in development.

Review the development process, standards, tools, tool options, and tool configurations at least **annually** to determine if the selected development processes, standards, tools, and configurations continue to satisfy the security and privacy requirements defined by the agency.

SA-15(3): Require the developer of the system, system component, or system service to perform a criticality analysis at key decision points defined by the agency as an input to the agency’s criticality analysis.

Developer-Supported Criticality Analysis

Agencies should require developers (internal or external), whether building full systems, components, or services, to conduct a criticality analysis as inputs to the agency's broader criticality assessment, helping to identify which elements are most essential to mission success, security, and operational continuity. This informs and strengthens the agency's own criticality analysis by providing technical insight from the development side.

317-11 Replace Unsupported System Components (SA-22)

End-of-life (EOL) software, firmware, and hardware shall be replaced when support for the components is no longer available from the developer, vendor, or manufacturer; or provide alternative sources for continued support such as in-house support, or support from external providers.

End-Of-Life & Unsupported System Components

Once a component reaches EOL, the manufacturer stops providing updates, patches, or technical assistance. Similarly, unsupported components are those that may still function but are no longer maintained or recognized by the vendor. Without vendor patches, vulnerabilities remain unaddressed, leaving systems exposed to cyber threats. All agencies shall track vendor lifecycle announcements to anticipate EOL dates and budget for replacements well before the vendor support ends.

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 800-161	Cybersecurity Supply Chain Risk Management	This document provides guidance on identifying, assessing, and mitigating risks associated with acquiring and integrating technology solutions.	*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
317-1	**Develop Agency-Level Procedures (SA-1)**	☐ Yes ☐ No
317-2	**Document the Allocation of Resources (SA-2)**	☐ Yes ☐ No
317-3	**Implement the System Development Life Cycle (SA-3)**	☐ Yes ☐ No
317-4	**Integrate Cybersecurity into the Acquisition Process (SA-4)**	☐ Yes ☐ No
317-5	**Maintain System Documentation (SA-5)**	☐ Yes ☐ No
317-6	**Require Alignment to Security and Privacy Engineering Principles (SA-8)**	☐ Yes ☐ No
317-7	**Require Secure External System Services (SA-9)**	☐ Yes ☐ No
317-8	**Require Developer Configuration Management (SA-10)**	☐ Yes ☐ No
317-9	**Require Developer Testing and Evaluation (SA-11)**	☐ Yes ☐ No
317-10	**Require Development Process, Standards, and Tools (SA-15)**	☐ Yes ☐ No
317-11	**Replace Unsupported System Components (SA-22)**	☐ 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.