State of Maryland

STANDARD

SUPPLY CHAIN RISK MANAGEMENT

Document No.	Last Updated	Prepared By
MD-STD-320-SR-01	02/18/2026	DOIT OSM

Cybersecurity Supply Chain Risk Management (C-SCRM), also simply referred to as Third Party Risk Management (TPRM), is critical to the State's operational resilience, minimizing the likelihood of a compromise to the State's technology and service supply chains.

PURPOSE AND SCOPE

Purpose	This standard provides the technical and operational specifications needed for procurement, development, and integration of secure systems and services.
Scope	This standard provides an organizational approach for managing the risks associated with the supply chain of information technology (IT) products, services, and service providers.
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

320 State Strategy

These standards establish a baseline of TPRM practices that each agency must implement to comply with State cybersecurity and privacy policies. TPRM practices prevent agencies from blindly trusting external vendors or third-party suppliers. Each agency shall designate specific personnel with IT responsibilities to ensure the effective implementation of these standards.

320-1 Develop Agency-Level Procedures (SR-1)

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

320-2 Develop a Supply Chain Risk Management Plan (SR-2)

Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of agency-procured/managed systems, system components or system services. Where feasible, include the following requirements in procurement review activities or pre-award due diligence activities:

- Assess supplier criticality and assign risk tiers, including documenting the potential impact of each supplier on mission and operational continuity;
- Conduct continuous monitoring of supplier security posture using automated risk monitoring throughout the vendor lifecycle (not limited to pre-award or onboarding activities);
- Use behavioral analytics and dynamic risk designation to assess third-party interactions;
- Require all supply chain entities to use multi-factor authentication (MFA) for authentication;
- Enforce immutable audit logs and cryptographic verification of software and hardware sources;
- Restrict supply chain entities to only necessary resources for their function;
- Require vendors to comply with State or agency-defined minimum-security requirements; and
- Isolate critical components from unverified supply chain elements.

Review and update the supply chain risk management plan **annually** or earlier if required to address threat, organizational, or environmental changes. Protect the SCRM plan from unauthorized disclosure and modification.

SR-2(1): Establish a formally chartered SCRM team consisting of the appropriate agency risk manager, IT/cybersecurity/privacy representative(s), procurement representative, and legal counsel to lead and support agency TPRM activities.

Enterprise vs Agency TPRM Plans

While State TPRM strategies are being developed and formalized, agencies can take proactive steps to implement localized techniques that reduce exposure and strengthen operational resilience. This includes: a) Conducting vendor risk assessments; b) Validating software provenance; and c) Enforcing minimum security requirements in procurement contracts. Agencies can also establish internal inventories of third-party dependencies, monitor for known vulnerabilities in supplied components, and apply threat intelligence to flag high-risk suppliers. By aligning these efforts with NIST SP 800-161 and other federal guidance, agencies contribute to a more secure ecosystem and ensure that agency practices are interoperable with the broader enterprise framework once fully deployed.

320-3 Develop Supply Chain Controls and Processes (SR-3)

Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements of agency systems or system components and incorporate any weaknesses in the agency risk management process for a risk decision from the appropriate Authorizing Official (AO). Employ the agency-defined supply chain controls to protect against supply chain risks to the system, system components, or system service and to limit the harm or consequences from supply chain-related events. Document the selected and implemented supply chain processes and controls in system security plans.

Supply Chain Controls & Processes

The NIST SP 800-161 Rev.1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations[2] provides more information about C-SCRM/TPRM best practices; When selecting and implementing security controls, verify agency alignment to the published catalog of Maryland Standards.

[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf

320-4 Employ Acquisition Strategies, Tools, and Methods (SR-5)

Employ acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks (e.g., vendor questionnaires, proposal evaluation criteria, and/or commercial risk rating tools).

Example Strategies, Tools, and Methods

Acquisition Type	Strategies, Tools, and Methods
Hardware	• Require a Hardware Bill of Materials (HBOM) for a detailed inventory of all components in a hardware product that may reveal untrusted parts before purchase. • Vet and monitor suppliers for financial stability, geopolitical exposure, and cybersecurity posture and diversify sourcing.
Software	• Require a Software Bill of Materials (SBOM) for a detailed inventory of all components, libraries, and dependencies in a software product that may reveal known vulnerabilities. • Verify secure development practices (e.g., Open Web Application Security Project (OWASP), NIST Secure Software Development Framework (SSDF)). • Limit and monitor third-party dependencies using tools that can flag outdated or vulnerable packages.
Services	• Conduct rigorous vendor due diligence looking for signs of overextension, recent layoffs, or acquisition activity. • Embed risk clauses in contracts to define measurable outcomes, response times, and escalation paths to protect against vendor failure or breach. • Diversify and build redundancy by qualifying backup vendors or multi-region service providers; or break large scopes into smaller, swappable components.

320-5 Perform Supplier Assessments and Reviews (SR-6)

Establish and maintain unique identification of systems or components deemed critical to the agency for tracking through the supply chain.

320-6 Establish Notification Agreements (SR-8)

Establish agreements and procedures with entities involved in the supply chain for the system, system components, or system service for the notification of supply chain compromises and results of assessments or audits consistent with State incident response policy and standards.

Reference MD-STD-308-IR for reporting timelines, escalation paths, and cross-agency coordination.

320-7 Inspect Systems or Components (SR-10)

Inspect agency critical systems or system components upon receipt of newly acquired equipment or upon indications of increased risk or equipment tampering using the below methods. Where feasible, agencies should use automated tools to detect tampering or firmware changes, especially for network-connected devices.

Common Inspection Methods

Method	Description
Visual Comparison	Use reference photos of original device condition; Look for changes in color, shape, or surface texture; and Check for overlays or 3D-printed components that mimic original parts.
Serial Number Verification	Match physical serial numbers with inventory records; and Confirm electronic serial number (via device interface) matches physical label.
Tamper-Evident Seals	Inspect for broken, missing, or replaced security seals; and Look for signs of peeling, scratches, or adhesive residue.
Loose or Missing Hardware	Check for loose screws, misaligned panels, or unusual gaps; Wiggle external components (e.g., card readers, universal serial bus (USB) ports) for unexpected movement.
Weight and Balance Check	Compare device weight against known baseline; Tampering may introduce hidden components like shimmers or rogue chips.
Cable and Connection Audit	Verify expected number, type, and color of cables; Look for unauthorized devices connected nearby (e.g., phones, USB drives).
Environmental Surveillance	Inspect surroundings for hidden cameras or suspicious objects; Check ceiling areas above terminals or workstations.

320-8 Verify Component Authenticity (SR-11)

Develop and implement anti-counterfeit procedures that include the means to detect and prevent counterfeit components from entering the system. Report counterfeit system components to the State Chief Information Security Officer (SCISO) and, if contractually permitted, notify the source of counterfeit components.

SR-11(1): Train agency staff with the responsibility of receiving and distributing IT to detect counterfeit system components (including hardware, software, and firmware) via OSM IT Manager training.

SR-11(2): Maintain configuration control over the systems and components deemed critical to the agency awaiting service or repair and serviced or repaired components awaiting return to service.

320-9 Establish Component Disposal Procedures (SR-12)

Dispose of state data, documentation, tools, systems, or system components using agency approved techniques and methods that align with MD-STD-310 Media Protection (MP) and maintain chain-of-custody documentation.

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 Practices for Systems and Organizations	This document provides guidance on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain.	*csrc.nist.gov (LINK)*
NIST SP 1326	Supply Chain Risk Management Due Diligence Assessment Quick-Start Guide	This guide provides C-SCRM/TPRM program capabilities with considerations for creating due diligence supply chain risk assessments in accordance with NIST Special Publication (SP) 800-161.	*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
320-1	**Develop Agency-Level Procedures (SR-1)**	☐ Yes ☐ No
320-2	**Develop a Supply Chain Risk Management Plan (SR-2)**	☐ Yes ☐ No
320-3	**Develop Supply Chain Controls and Processes (SR-3)**	☐ Yes ☐ No
320-4	**Employ Acquisition Strategies, Tools, and Methods (SR-5)**	☐ Yes ☐ No
320-5	**Perform Supplier Assessments and Reviews (SR-6)**	☐ Yes ☐ No
320-6	**Establish Notification Agreements (SR-8)**	☐ Yes ☐ No
320-7	**Inspect Systems or Components (SR-10)**	☐ Yes ☐ No
320-8	**Verify Component Authenticity (SR-11)**	☐ Yes ☐ No
320-9	**Establish Component Disposal Procedures (SR-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.