Division of Enterprise Technology Strategy and Services

ETSS Policy 800.2

Supply Chain Risk Management Policy (SR)

Publish Date: 15 July 2026
Effective Date: 15 July 2026
Last Revision Date: 14 July 2026

doa.entsec@doit.ri.gov

1. Purpose

This policy establishes the requirements for identifying, assessing, and mitigating risks associated with the information and communications technology (ICT) supply chain. Supply chain risk management (SCRM) addresses risks introduced through the development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of information systems, system components, and system services. This policy extends beyond procurement activities to encompass the full lifecycle of supply chain risk, including counterfeit detection, component authenticity, and supplier security oversight.

This policy supports the State's compliance with NIST SP 800-53 Revision 5 (Supply Chain Risk Management family), NIST SP 800-161 (Cybersecurity Supply Chain Risk Management Practices), NIST Cybersecurity Framework 2.0, IRS Publication 1075, and other applicable federal and state regulatory requirements. This policy should be read in conjunction with the ETSS System and Services Acquisition Policy (800.x).

2. Applicability

This policy applies to all State of Rhode Island Executive Branch departments, including agencies, boards, and commissions, as well as their employees (permanent, non-permanent, full-time, and part-time), interns, consultants, contractors, vendors, and any entity that has access to State information systems and data, whether operated or maintained by the State or on behalf of the State. For the purposes of this policy, the term "Agency" refers to any department, agency, division, or unit of the Executive Branch.

This policy applies to all IT acquisitions and supply chain activities, including commercial off-the-shelf (COTS) products, custom-developed systems, externally hosted systems, cloud services, and contracted development and operations services.

3. Definitions

The following terms are defined for the purposes of this policy. All other terms should be referenced in the ETSS Glossary of Terms, Acronyms, and Definitions.

Supply Chain Risk Management (SCRM)

A systematic process for managing supply chain risk by identifying susceptibilities,

vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats. SCRM addresses risks presented by the supplier, the supplied product and its subcomponents, and the supply chain itself, including production, packaging, handling, storage, transport, operations, and disposal. SCRM encompasses and extends beyond the procurement activities of the ETSS Vendor Management Office (VMO).

Counterfeit Component

An unauthorized copy, imitation, substitute, or modified component that is knowingly misrepresented as a genuine component from the original manufacturer or authorized distributor. Counterfeit components may compromise the integrity, reliability, and security of information systems.

Trusted Distribution Channel

A verified and authenticated supply path from the original equipment manufacturer (OEM) or authorized distributor to the acquiring organization, used to reduce the risk of product tampering, substitution, or counterfeiting during transit.

4. Procedures for Compliance

The following requirements establish the supply chain risk management controls that agencies and ETSS must implement. Security controls are assigned based on the Information Assurance Level (IAL) of the information system, aligned to the NIST SP 800-53 Rev. 5 Moderate baseline.

4.1 Supply Chain Risk Management Policy and Procedures (SR-1)

Applies to: All systems (IAL1, IAL2)

Each agency shall develop, document, and disseminate a supply chain risk management policy and supporting procedures to designated personnel identified in the applicable System Security Plan. The ETSS Chief of the Vendor Management Office (VMO) is designated as the official responsible for the enterprise SCRM policy. The policy shall be reviewed and updated at least every three (3) years and following significant changes. Supporting procedures shall be reviewed in alignment with the policy.

4.2 Supply Chain Risk Management Plan (SR-2)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Develop a SCRM plan for managing supply chain risks associated with the development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of information systems, system components, and system services. The SCRM plan may be a standalone document or incorporated into system security plans. The plan shall define requirements for vendor due diligence and onboarding, security and privacy control expectations, contractual security requirements and right-to-audit provisions, and ongoing vendor risk oversight.

b. Review and update the SCRM plan at least annually to address current threats or changes within the agency, supply chain, or operational environments.

c. Protect the SCRM plan from unauthorized disclosure or modification.

4.2.1 Establish SCRM Team (SR-2(1))

Applies to: All systems (IAL1, IAL2)

Each agency shall establish a SCRM team comprised of personnel with roles and responsibilities necessary to lead and support SCRM and SDLC activities. The team shall include, as appropriate, leadership from ETSS infrastructure, operations, and security teams, the ETSS Vendor Management Office (VMO), the ETSS Portfolio and Project Management Office (PPMO), Purchasing, Legal, Agency Information Managers (AIMs), agency Technical Support Managers (TSMs), and agency executives responsible for risk, security, and privacy. The team shall

provide expertise in acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as the technical aspects and dependencies of information systems.

4.3 Supply Chain Controls and Processes (SR-3)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Establish a process to identify and address weaknesses or deficiencies in supply chain elements and processes of critical information systems in coordination with ETSS supply chain personnel. This includes hardware, software, and firmware development processes, shipping and handling procedures, personnel and physical security programs, configuration management tools, and other programs associated with the development, acquisition, maintenance, and disposal of systems and system components.

b. Employ controls, including the identification of alternate vendors and suppliers, to protect against supply chain risks and to limit the harm or consequences from supply chain-related events.

c. Document the selected and implemented supply chain processes and controls within applicable system security plans and associated SCRM documents.

4.4 Acquisition Strategies, Tools, and Methods (SR-5)

Applies to: All systems (IAL1, IAL2)

Each agency shall employ acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks. Agencies shall follow the processes outlined by the VMO for project intake as established by ETSS IT Approval Policy (850.x) to ensure cyber and operational risk considerations are identified and treated. Strategies shall include the use of tamper-evident packaging and trusted distribution channels. Acquisition contracts shall include security requirements per the ETSS System and Services Acquisition Policy (800.x), including FIPS-validated cryptography, patch management commitments, vulnerability disclosure, and incident reporting. High-value or sensitive system acquisitions may require independent security assessments or certifications as a contract condition.

4.5 Supplier Assessments and Reviews (SR-6)

Applies to: Moderate and above (IAL2)

Each agency shall assess and review supply chain-related risks associated with suppliers or contractors and the information systems, system components, or services they provide at initial procurement and at each contract renewal cycle thereafter (annually by default if no renewal cycle is defined), or after a serious security incident at the supplier or involving supplier systems. Supply chain risk assessments shall be conducted within the enterprise Governance, Risk, and Compliance (GRC) platform by the ETSS CISO or authorized delegate. Supplier assessments shall include, as appropriate:

a. Inbound material assessments to ensure parts and materials conform to supplier requirements.

b. Functional development assessments to verify SDLC practices, tool adequacy, trade secret protection, and testing of design changes.

c. Enterprise and IT assessments to verify network and system security, physical access controls, supplier support commitments for the expected life of the system, and the existence and testing of business continuity plans.

d. Manufacturing process assessments for compliance with ISO and industry standards, change authorization, and testing of completed goods.

e. Outbound goods assessments to verify adequate spares and absence of tampering, product substitution, or counterfeiting.

f. Risk management assessments addressing malicious software, known vulnerabilities, insecure coding practices, supply chain risk management maturity, and security controls.

4.6 Notification Agreements (SR-8)

Applies to: All systems (IAL1, IAL2)

Each agency shall establish agreements and procedures with entities involved in the supply chain for the notification of supply chain compromises (actual or potential) and the sharing of security audit or assessment results, in accordance with the ETSS Incident Response Plan and contract or SLA requirements.

4.7 Inspection of Systems or Components (SR-10)

Applies to: All systems (IAL1, IAL2)

Each agency shall inspect the information system or system component upon:

a. Initial receipt or delivery of the system or component.

b. Return of the system or component to the agency after each occurrence that the system or component is removed from a controlled area.

c. Detection of evidence of actual or potential tampering.

4.8 Component Authenticity (SR-11)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Develop and implement anti-counterfeit policies and procedures to detect and prevent counterfeit components from entering the network and information systems. Hardware and software components shall be obtained from original equipment manufacturers (OEMs), authorized resellers, or the General Services Administration (GSA) schedule to reduce counterfeiting risk. At a minimum, IT-related anti-counterfeit procedures shall: (1) require suppliers, vendors, and contractors to notify the VMO and program managers when critical items are not obtained from OEMs or authorized distributors; (2) require program managers to perform a risk assessment evaluating the counterfeit risk of mission-critical systems or components; (3) for components not received from the original manufacturer or authorized distributor, require program managers to implement a process to test and verify authenticity; and (4) for suspected counterfeit systems or components, require program managers to contact the Chief of VMO, Chief of I&O, and CISO within one (1) business day, with the suspected component not placed on the State network without prior CISO approval.

b. Report counterfeit information systems or components to the source of the counterfeit component, CISA, the agency Director, AIM, TSM, system owner, ETSS CDO, ETSS CISO, and other personnel requiring notification, as appropriate.

4.8.1 Anti-Counterfeit Training (SR-11(1))

Applies to: All systems (IAL1, IAL2)

Each agency shall train all system support personnel, including procurement personnel, system administrators, network administrators, database administrators, and staff responsible for installing hardware components, to detect counterfeit information systems or components. Anti-counterfeiting awareness shall be incorporated into relevant role-based security training in accordance with the ETSS Awareness and Training Policy (950.x).

4.8.2 Configuration Control for Component Service and Repair (SR-11(2))

Applies to: All systems (IAL1, IAL2)

Each agency shall maintain configuration control over information system components awaiting service or repair, as well as serviced or repaired components

awaiting return to service, in accordance with ETSS configuration management, system maintenance, and developer requirements.

4.9 Component Disposal (SR-12)

Applies to: All systems (IAL1, IAL2)

Suppliers shall dispose of data, documentation, tools, and system components associated with the information system, system component, or system service being provided to the agency in accordance with ETSS policies and procedures and industry best practices. See the ETSS Media Protection Policy (300.x) for sanitization and disposal requirements.

5. Repercussions for Non-Compliance

Failure to comply with this policy may result in corrective action proportional to the severity of the violation. Consequences may include, but are not limited to:

a. Suspension or termination of vendor or contractor agreements for non-compliant supply chain partners.

b. Denial of system authorization for systems acquired through non-compliant supply chain processes.

c. Mandatory remediation of supply chain deficiencies within defined timelines.

d. Referral to agency management for disciplinary proceedings for personnel who bypass supply chain risk management requirements.

e. Referral to law enforcement if counterfeit components, product tampering, or fraudulent supply chain activity is suspected.

Non-compliance findings shall be documented and tracked through ETSS governance processes and may be recorded as findings in the agency Plan of Action and Milestones (POAM).

6. Roles and Responsibilities

The following roles are accountable for the implementation, monitoring, and enforcement of this policy:

ETSS Chief of the Vendor Management Office (VMO)

Designated as the official responsible for the enterprise SCRM policy and the SCRM Plan. Manages the vendor due diligence and onboarding process, oversees contractual security requirements, coordinates supplier assessments and reviews, maintains the enterprise list of service providers, and leads anti-counterfeit procurement controls. Receives notification of critical items not obtained from OEMs or authorized distributors.

Chief Information Security Officer (CISO)

Conducts or delegates supply chain risk assessments within the enterprise GRC platform. Receives notification of suspected counterfeit components within one business day. Approves placement of suspected counterfeit components on the State network (or deny placement). Coordinates incident response for supply chain compromises and counterfeit detections. Reports confirmed counterfeit findings to external organizations as required.

Chief Digital Officer (CDO)

Receives notification of confirmed counterfeit findings. Provides executive oversight of supply chain risk management as part of the enterprise risk governance structure.

Chief of Infrastructure and Operations (I&O)

Receives notification of suspected counterfeit components. Supports component inspection, authentication testing, and configuration control for components awaiting or returning from service and repair.

SCRM Team

A cross-functional team comprising ETSS infrastructure, operations, and security leadership, VMO, Portfolio and Project Management Office, Purchasing, Legal, AIMs, TSMs, and agency

executives. Leads and supports SCRM and SDLC activities, provides expertise in acquisition, legal, and technical domains.

System Owners

Responsible for ensuring supply chain risk management controls are implemented for their systems, coordinating supplier assessments for system-specific acquisitions, and maintaining configuration control over components during service and repair.

Agency Information Managers (AIMs) / Technical Support Managers (TSMs)

Coordinate supply chain risk management activities at the agency level, receive notification of counterfeit component findings, and participate in the SCRM team.

7. Approval / Review Signatures

Ramesh madhavan

Digitally signed by Ramesh madhavan
Date: 2026.07.15 08:29:48 -04'00'

Chief, IT Vendor Management (VMO)
Division of Enterprise Technology Strategy and Services

Digitally signed by Nathan Loura
Date: 2026.07.15 10:51:38 -04'00'

Chief Information Security Officer (CISO)
Division of Enterprise Technology Strategy and Services

Brian Tardiff

Digitally signed by Brian Tardiff
Date: 2026.07.15 11:29:56 -04'00'

Chief Digital Officer (CDO)
Division of Enterprise Technology Strategy and Services