Nuclear Regulatory Commission
Office of the Chief Information Officer

Supply Chain Risk Management Strategy

Revision Number:	1.0
Primary Contact:	Kathy Lyons-Burke Senior Level Advisor for Information Security
Responsible Organization:	Supply Chain Risk Management Governance Board
ADAMS Accession #:	ML20177A361

Effective Date:	01-Mar-2022	**Signature and Date**
Approved By:	David Nelson Chief Information Officer	David J. Nelson Digitally signed by David J. Nelson Date: 2022.02.03 08:34:28 -05'00'
	Sherri Miotla (Acting) Performance Improvement Officer[1]	Cheryl A. Miotla Digitally signed by Cheryl A. Miotla Date: 2022.02.02 14:01:58 -05'00'

[1] At the NRC, the Performance Improvement Officer performs duties including those of a Chief Risk Officer

Table of Contents

Supply Chain Risk Management Strategy

1 PURPOSE

This document provides the agency strategy for supply chain risk management.

2 BACKGROUND

In 2008, counterfeit Cisco networking gear was found in U.S. government networks, allowing unauthorized access to the networks. In response to this threat, the National Institute of Standards and Technology (NIST) updated Special Publication (SP) 800-53, revision 4 "Security and Privacy Controls for Federal Information Systems and Organizations" in 2013 to include supply chain cybersecurity controls; provided SP 161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations" in 2015 to further address cybersecurity supply chain risks; and added additional supply chain controls to the draft of SP 800-53, revision 5. In 2016, the Office of Management and Budget (OMB) added supply chain considerations to Circular A-130, "Managing Information as a Strategic Resource." In 2018, the Government Accountability Office (GAO) testified before the Subcommittees on Counterterrorism and Intelligence, and Oversight and Management Efficiency, Committee on Homeland Security, House of Representatives on Supply Chain Risks Affecting Federal Agencies, and the "Federal Acquisition Supply Chain Security Act of 2018" was placed into law, creating a Federal Acquisition Security Council (FASC) to provide federal acquisition security and supply chain risk management guidance.

In February of 2020, GAO examined the extent to which agencies have implemented foundational practices for managing Information and Communications Technology (ICT) supply chain risks, and NRC was one of the agencies examined against the NIST SP 800-161 identified Supply Chain Risk Management (SCRM) practices. GAO found that NRC has not implemented any of the ICT SCRM foundational practices (provided in Appendix C).

3 APPROACH

This strategy uses the documents identified in the background section for the strategy to address supply chain risks. The document organization follows the tiers identified in NIST SP 800-161:

- Tier 1
  - Development of the overall ICT SCRM strategy (this document).
  - Determination of organization-level ICT SCRM risks.
  - Setting agency-wide ICT SCRM policies to guide the organization's activities in establishing and maintaining organization-wide ICT SCRM capability.
- Tier 2
  - Prioritizing the agency's mission and business functions.
  - Conducting mission/business-level risk assessment.
  - Implementing Tier 1 strategy and guidance to establish an overarching organizational capability to manage ICT supply chain risks.

  - Guiding organization-wide ICT acquisitions and their corresponding SDLCs.
- Tier 3
  - Specific ICT SCRM activities applied to individual information systems and information technology acquisitions, including integration of ICT SCRM into these systems' SDLCs.

4 TIER 1 – ORGANIZATION

This tier includes development of the agency SCRM strategy (this document), analysis of existing and potential supply chain risks, and identifying how the agency will manage supply chain risks.

4.1 ICT SCRM Policy

The Chief Information Officer (CIO) will work collaboratively with the Chief Acquisition Officer (CAO) to identify needed modifications to the ICT acquisition methodology to address SCRM.

The Office of the Chief Information Officer (OCIO) and Office of Administration (ADM) will incorporate high-level requirements and responsibilities for ICT SCRM into Management Directive (MD) 12.5, "NRC Cybersecurity Program" and MD 11.1, "NRC Acquisition of Supplies and Services" respectively.

4.2 ICT SCRM Governance

The agency will establish an agency-wide executive governance board to identify the level of supply chain risk the agency will accept, and how the agency will assess (e.g., acceptable risk assessment methodologies), respond to (e.g., acceptance, mitigation, avoidance), and monitor ICT supply chain risks across the life cycle of ICT products and services. The SCRM executive governance board shall include at a minimum, the CIO, CAO, Performance Improvement Officer, Chief Financial Officer (CFO), Director of the Office of Nuclear Reactor Regulation (NRR), Director of the Office of Nuclear Material Safety and Safeguards (NMSS), and the Director of Office of Nuclear Security and Incident Response (NSIR), with an Office of General Counsel (OGC) representation. The agency will ensure that activities required to support ICT SCRM are resourced as needed.

The SCRM executive oversight board will establish an SCRM working group to perform the following:

- Identify mission/business requirements that impact the agency's approach to SCRM. These requirements include, but are not limited to, cost, schedule, performance, security, privacy, quality, and safety.
- Identify security requirements relevant to SCRM.
- Identify mission/business functions impacted by SCRM.
- Modify/create agency processes and procedures to address SCRM.
- Identify contract language that must be included in all acquisitions that have an ICT component that is required to perform the contracted activities.
- Ensure that Trade Agreement Act (TAA) compliance is incorporated into all acquisitions.

4.3 Risk Management

OCIO will update CSO-PROS-2030, “NRC Risk Management Framework (RMF) and Authorization Process” to reflect current laws and federal guidance, identify how and how often an ICT SCRM agencywide risk assessment is performed, and how quality assurance and quality control are addressed with respect to SCRM. OCIO will also update the following processes and procedures to include SCRM:

- CSO-PROC-2104, “System Artifact Examination Procedure”
- CSO-PROS-1323, “Information Security Continuous Monitoring Process”
- CSO-PROS-2102, “System Cybersecurity Assessment Process”

OCIO will update system security plan templates to incorporate ICT SCRM Plan components identified in NIST SP 800-161.

4.4 ICT SCRM Roles and Responsibilities

The SCRM executive governance board and working group will identify SCRM roles and responsibilities, including for the following:

- Who is responsible and has authority for taking actions related to SCRM acquisitions, incidents, and risk management.
- Who is accountable for SCRM decisions.
- Who will be consulted and informed should an SCRM issue arise.

4.5 Supplier Management Program

The agency will implement a supplier management program led by the CAO and the Senior Agency Official for Supply Chain Risk Management (SAOSCRM). The CAO and SAOSCRM, in coordination with the SCRM executive governance board, will establish guidelines for purchasing that address SCRM, including preference for purchasing directly from qualified original equipment manufacturers (OEMs) or their authorized distributors and resellers, and an approach to identify and document agency ICT supply chains that includes information relevant to the supply chain, such as suppliers, manufacturing facilities, logistics providers, distribution centers, distributors, wholesalers, and other organizations involved in the manufacturing, operation, management, processing, design and development, handling, and delivery of products and services.

The CAO and SAOSCRM, in coordination with the SCRM executive governance board, will also establish a process for conducting reviews of potential suppliers to identify risks associated with the potential use of suppliers (and their subordinate suppliers) prior to selecting products and services. The process will include the ability to leverage other federally accepted supply chain risk reviews.

4.6 Incident Management

The CIO will ensure that the agency incident management program includes relevant processes and procedures related to SCRM, including identification of incidents caused by supply chain issues and managing those incidents.

4.7 Internal Checks and Balances

OCIO will develop processes and procedures to detect counterfeit and compromised ICT products prior to their deployment.

5 TIER 2 – MISSION/BUSINESS PROCESS

This tier uses risk context, risk decisions, and risk activities identified in Tier 1 to address risk from a mission/business perspective and defines program requirements for SCRM. Mission/business processes and procedures are modified to address relationships with system integrators, suppliers, and external service providers with respect to SCRM.

5.1 Risk Management

Mission/business process owners will modify those processes to include ICT SCRM considerations, including supply chain risk identification and management.

OCIO will integrate ICT SCRM requirements into the agency enterprise architecture to facilitate the allocation of ICT SCRM controls to agency information systems and the environments in which those systems operate.

5.2 Risk Assessment Processes

OCIO will update processes used to assess risk to incorporate a supply chain risk assessment.

6 TIER 3 – INFORMATION SYSTEMS

This tier is where SCRM is integrated into the System Development Life Cycle (SDLC).

6.1 Risk Management

Each system owner will ensure that the system security plan incorporates ICT SCRM Plan components identified in NIST SP 800-161.

6.2 Baseline Information Security Controls

Each system owner will ensure that the system baseline security controls include the SCRM controls identified in NIST SP 800-161.

6.3 Contingency Plan

Each system owner will ensure that the system contingency plan incorporates supply chain risk considerations and contingency plan tests address those considerations.

6.4 Incident Management

Each system owner will ensure development of incident management processes and procedures that address identification of supply chain related incidents and notification of the agency Computer Security Incident Response Team (CSIRT).

APPENDIX A ACRONYMS

ADM	Office of Administration
CAO	Chief Acquisition Officer
CIO	Chief Information Officer
COTS	Commercial off the Shelf
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
EO	Executive Order
FASC	Federal Acquisition Security Council
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FITARA	Federal Information Technology Acquisition Reform Act
GAO	Government Accountability Office
ICT	Information and Communications Technology
MD	Management Directives
NIST	National Institute of Standards and Technology
NMSS	Office of Nuclear Material Safety and Safeguards
NRR	Office of Nuclear Reactor Regulation
NSIR	Office of Nuclear Security and Incident Response
NVD	National Vulnerability Database
OCIO	Office of the Chief Information Officer
OGC	Office of General Counsel
OEM	Original Equipment Manufacturers
OMB	Office of Management and Budget
RMF	Risk Management Framework

SAOSCRM	Senior Agency Official for Supply Chain Risk Management
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SP	NIST Special Publication
TAA	Trade Agreement Act

APPENDIX B REFERENCES

Executive Order (EO)

EO 13806, “Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States,” September 2018.

EO 13873, “Securing the Information and Communications Technology and Services Supply Chain,” May 15, 2019.

Government Accountability Office (GAO)

GAO Statement of Facts – ICT Supply Chain Cybersecurity (103187)

National Institutes of Standards and Technology

NIST Computer Security Division, Computer Security Resource Center:
http://csrc.nist.gov

NIST Federal Information Processing Standards (FIPS) Publications:
http://csrc.nist.gov/publications/PubsFIPS.html

NIST Publications:
http://csrc.nist.gov/publications/

NIST SP 800-30, “Guide for Conducting Risk Assessments”

NIST SP 800-37, “Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach.”

NIST SP 800-39, “Managing Information Security Risk”

NIST SP 800-53, Draft Rev. 5, “Security and Privacy Controls for Federal Information Systems and Organizations”

NIST SP 800-53, Rev. 4, “Security and Privacy Controls for Federal Information Systems and Organizations”

NIST SP 800-161, “Supply Chain Risk Management Practices for Federal Information Systems and Organizations.”

Nuclear Regulatory Commission Documents

Management Directives (MD)

MD 12, “Glossary of Security Terms”

MD 11.1, “NRC Acquisition of Supplies and Services”

MD 12.5, “NRC Cybersecurity Program”

Office of Management and Budget Documents (OMB)

OMB Circular A-130, “Managing Information as a Strategic Resource,” July 28, 2016

United States Code

Federal Acquisition Supply Chain Security Act of 2018 (41 U.S.C. 1322).

Federal Information Security Modernization Act (FISMA) of 2014 (44 U.S.C. 3541 et seq.).

Federal Information Technology Acquisition Reform Act (FITARA), Pub. L. 113 291.

Trade Agreement Act (TAA) (19 U.S.C. & 2501-2581)

APPENDIX C NIST SP 800-161 ICT SCRM PRACTICES

Implement a risk management hierarchy and risk management process (in accordance with NIST SP 800-39, Managing Information Security Risk [NIST SP 800-39]) including an organization-wide risk assessment process (in accordance with NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments).

Establish an organization governance structure that integrates ICT SCRM requirements and incorporates these requirements into the organizational policies.

Establish consistent, well-documented, repeatable processes for determining [FIPS 199] impact levels.

Use risk assessment processes after the [FIPS 199] impact level has been defined, including criticality analysis, threat analysis, and vulnerability analysis.

Implement a quality and reliability program that includes quality assurance and quality control process and practices.

Establish a set of roles and responsibilities for ICT SCRM that ensures that the broad set of appropriate stakeholders are involved in decision making, including who has the required authority to take action, who has accountability for an action or result, and who should be consulted and/or informed (e.g., Legal, Risk Executive, HR, Finance, Enterprise IT, Program Management/System Engineering, Information Security, Acquisition/procurement, supply chain logistics, etc.).

Ensure that adequate resources are allocated to information security and ICT SCRM to ensure proper implementation of guidance and controls.

Implement consistent, well-documented, repeatable processes for system engineering, ICT security practices, and acquisition.

Implement an appropriate and tailored set of baseline information security controls in NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

Establish internal checks and balances to assure compliance with security and quality requirements.

Establish a supplier management program including, for example, guidelines for purchasing directly from qualified original equipment manufacturers (OEMs) or their authorized distributors and resellers.

Implement a tested and repeatable contingency plan that integrates ICT supply chain risk considerations to ensure the integrity and reliability of the supply chain including during adverse events (e.g., natural disasters such as hurricanes or economic disruptions such as labor strikes).

Implement a robust incident management program to successfully identify, respond to, and mitigate security incidents. This program should be capable of identifying causes of security incidents, including those originating from the ICT supply chain.

Supply Chain Risk Management Strategy Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
31-Jan-22	1.0	Initial draft	Distribution to the SCRM GB	None