Nuclear Regulatory Commission

Supply Chain Risk Management Governance Board Charter

Revision Number:	1.0
Primary Contact:	Kathy Lyons-Burke Senior Level Advisor for Information Security
Responsible Organization:	OCIO
ADAMS Accession #:	ML21074A023

Effective Date: 15-Jun-2021

Approved By: David Nelson
Chief Information Officer

David J. Nelson
Digitally signed by David J. Nelson
Date: 2021.06.29 15:25:01 -04'00'

Catherine Haney
Performance Improvement Officer[1]

Catherine Haney
Digitally signed by Catherine Haney
Date: 2021.07.26 13:38:31 -04'00'

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

Table of Contents

Supply Chain Risk Management Governance Board Charter

1 PURPOSE

The Supply Chain Risk Management (SCRM) governance board is a body comprised of senior-level staff and is being established to ensure that the U.S. Nuclear Regulatory Commission (NRC) is performing supply chain risk management in accordance with NRC mission needs and relevant laws, regulations, executive orders, and directives.

2 MEMBERSHIP

The SCRM governance board (SCRMGB) is co-chaired by the NRC's Senior Agency Official for Supply Chain Risk Management (SAOSCRM) and Performance Improvement Officer. The membership is as follows:

Voting Members or Positions	**Title(s)**
Director, Office of the Chief Information Officer	Chief Information Officer (CIO) / SAOSCRM
Executive Director for Operations (EDO) Assistant for Operations	Performance Improvement Officer
Director, Office of the Chief Financial Officer	Chief Financial Officer (CFO)
Director, Office of Administration (ADM)	Chief Acquisition Officer (CAO)
Director, Office of Nuclear Material Safety and Safeguards	Supply Chain Risk Management Agency Official
Director, Office of Nuclear Reactor Regulation	Supply Chain Risk Management Agency Official
Director, Office of Research	Supply Chain Risk Management Agency Official
Director, Office of Nuclear Security and Incident Response	Supply Chain Risk Management Agency Official
Advisory Members[2]	**Title(s)**
Office of the General Counsel	General Counsel
Chief Information Security Officer (CISO)	CISO
ADM, Acquisition Management Division Director	Acquisition Management Division Director

[2] The advisory member position in the Office of the General Counsel may be represented by a designee at SCRMGB meetings

3 DEFINITIONS

ICT Supply Chain	A linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.
ICT Supply Chain Risk	Risks that arise from the insertion of counterfeits, unauthorized production, tampering, theft; insertion of malicious software and hardware (e.g., GPS tracking devices, computer chips, etc.); as well as poor manufacturing and development practices in the ICT supply chain that could results in loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
ICT Supply Chain Risk Management	The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of information and communications technology product and service supply chains.

4 RESPONSIBILITIES

This section identifies responsibilities associated with governance board membership. Responsibilities of the Supply Chain Risk Management Governance Board Co-chairs

4.1 Responsibilities of the Supply Chain Risk Management Governance Board Co-chairs

The responsibilities of the SCRMGB Co-chairs include, but are not limited to, the following:

1. Fulfill the required functions for supply chain risk management delineated laws, regulations, executive orders, and directives.
2. As the lead for the agency's SCRMGB, the duties of the co-chairs or designee include the following:
    a. Establish meetings and agendas.
    b. Schedule meetings and distribute meeting materials.
    c. Record and distribute the meeting minutes.
    d. Communicate the SCRMGB's decisions to appropriate stakeholders.

4.2 Responsibilities of the Supply Chain Risk Management Governance Board

The responsibilities of the SCRMGB include, but are not limited to, the following:

1. Maintain an overall Information and Communications Technology (ICT) SCRM strategy.
2. Determine agency ICT SCRM risks and develop Enterprise Risk Reports.

3. Ensure ICT SCRM risks are addressed appropriately.
4. Establish agencywide ICT SCRM policies and guidance to guide the organization's activities in establishing and maintaining an organization-wide ICT SCRM capability.
5. Identify the level of supply chain risk the agency finds acceptable, and how the agency assesses (e.g., acceptable risk assessment methodologies), responds to (e.g., acceptance, mitigation, avoidance), and monitors ICT supply chain risks across the life cycle of ICT products and services.
6. Implement supply chain risk management principles to protect against the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software, as well as poor manufacturing and development practices throughout the system development life cycle.
7. Ensure review of system owner developed supply chain risk management plans as described in NIST SP 800-161 and other standards that include supply chain risk management relevant controls to ensure the integrity, security, resilience, and quality of information systems, and development of an agency risk assessment based upon those plans.
8. Establish an SCRM working group to perform the following:
    a. 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.
    b. Identify security requirements relevant to SCRM.
    c. Identify mission/business functions impacted by SCRM.
    d. Modify/create agency processes and procedures to address SCRM.
    e. Identify contract language that must be included in all acquisitions to perform required SCRM.
    f. Ensure that Trade Agreement Act (TAA) compliance is incorporated into all acquisitions.

The advisory member positions may be represented by a designee at SCRMGB meetings.

4.3 Responsibilities of the Senior Agency Official for Supply Chain Risk Management

The responsibilities of the SAOSCRM include the following:

1. In coordination with the CAO:
    a. Ensure that the ICT acquisition methodology adequately addresses SCRM.
    b. 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.
    c. 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.

4.4 Responsibilities of the Chief Information Officer

The responsibilities of the CIO include the following:

1. Ensure that supply chain risk management policy is reflected in Management Directive (MD) 12.5, “NRC Cybersecurity Program.”
2. Ensure development of processes and procedures to detect counterfeit and compromised ICT products prior to their deployment.
3. Ensure ICT SCRM requirements are integrated 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.
4. Ensure processes used to assess risk incorporate a supply chain risk assessment.

4.5 Responsibilities of the Chief Acquisition Officer

The responsibilities of the CAO include the following:

1. Ensure that supply chain risk management policy is reflected in Management Directive (MD) 11.1, “NRC Acquisition of Supplies and Services.”
2. In coordination with the SAOSCRM:
    a. Ensure that the ICT acquisition methodology adequately addresses SCRM.
    b. 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.
    c. 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.
3. Ensure that NRC acquisitions make use of adequate competition, analyze risks (including supply chain risks) associated with potential contractors and the products and services they provide, and allocate risk responsibility between Government and contractor when acquiring IT.

4.6 Responsibilities of the Chief Financial Officer

The CFO is responsible for ensuring that activities required to support ICT SCRM are resourced as needed.

4.7 Responsibilities of the Performance Improvement Officer

The Performance Improvement Officer is responsible for identifying the acceptable level of risk for enterprise and mission activities.

5 METHODS AND PROCEDURES

The SCRMGB uses the following methods and procedures.

5.1 Meetings

The SCRMGB meets on a quarterly basis or as often as necessary to accomplish its purpose.

The NRC's SCRM Working Group briefs the SCRMGB on the status of actions and activities and presents recommendations to the SCRMGB for voting.

5.2 Meeting Ground Rules

Voting is conducted based on the members present but must include the voting member(s) impacted by the decision. Members must be notified of any proposed items for vote prior to a meeting. Members have the right to abstain from voting. The Co-Chairs take into consideration all positions presented and the outcome of the votes to make a final decision. The Co-Chairs capture member votes, including the final decision made by the Co-Chairs, and record the information in the meeting minutes.

5.3 Meeting Minutes

The Co-Chairs' designee prepares the draft meeting minutes, stores the draft meeting minutes on the SCRMGB Microsoft (MS) Teams site, and distributes a link to the members electronically using e-mail. Members may provide comments or corrections to the minutes for 2 weeks after the draft minutes have been distributed. The final minutes are saved on the SCRMGB MS Teams site with a link distributed to the membership through e-mail and stored as a permanent record in NRC's Agencywide Documents Access and Management System.

5.4 Communications

The Co-Chairs designee distributes meeting invitations, agendas, documents to review, and other notices to each member by e-mail.

5.5 Quarterly Performance Reviews

The Co-Chairs provide information about notable SCRM risks for discussion at agency quarterly performance reviews.

Supply Chain Risk Management Governance Board Charter Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
01-Jun-21	1.0	Initial draft		