NNSA POLICY

NAP 540.4

Approved: 01-21-2026
Certification Due: 01-21-2031

SUPPLY CHAIN RISK MANAGEMENT (SCRM)

National Nuclear Security Administration

NATIONAL NUCLEAR SECURITY ADMINISTRATION
Office of Partnership and Acquisition Services

THIS PAGE INTENTIONALLY LEFT BLANK

SUPPLY CHAIN RISK MANAGEMENT (SCRM)

1. PURPOSE. To establish supply chain risk management (SCRM) policy for the National Nuclear Security Administration's (NNSA) nuclear security enterprise (NSE).

2. AUTHORITY. This NNSA Policy (NAP) is written under the Administrator's authority to set policy established pursuant to 50 United States Code (U.S.C.) 2402(d).

3. CANCELLATION. None.

4. APPLICABILITY.

   a. Federal. This NAP applies to all Federal NNSA elements.

   b. Contractors. The Contractor Requirements Document (CRD), provided separately as Attachment 1, sets forth requirements that apply to management and operating (M&O) contractors. The CRD is marked Controlled Unclassified Information (CUI) and can be acquired by contacting the NNSA Office of Partnership and Acquisition Services. It must be included in NNSA M&O contracts.

   c. Equivalencies/Exemptions.

      (1) Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 U.S.C. 2406 and 2511, and to ensure consistency throughout the joint Navy/Department of Energy (DOE) Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.

      (2) Exemptions. None.

5. SUMMARY OF CHANGES. Not applicable.

6. BACKGROUND. Mitigating supply chain risks and ensuring supply chain integrity, availability, and resiliency is a strategic imperative for NNSA. Successful SCRM requires long-term collaboration across the NSE. This policy establishes criteria for supply chain vetting, information sharing, risk management, and reporting.

7. REQUIREMENTS.

   NNSA must manage supply chains risks associated with procurement of products and services by:

      (1) Vetting potential suppliers for supply chain risks prior to solicitation or contract award;

(2) Identifying and understanding relevant supply chain information and associated risks to inform decision-making.

(3) Determining supply chain risk impacts due to control or influence from foreign ownership.

(4) Sharing supplier risk assessments (SRA) and risk information with NSE laboratories, plants, sites, and program offices to the maximum possible.

(5) Acknowledging and mitigating supplier risks or applying appropriate controls or strategies; and

(6) exercising actions under the Enhanced Procurement Authority (EPA) (see 50 U.S.C. 2786) or authority of the *Federal Acquisition Supply Chain Security Act* of 2018 (FASCSA) (see 41 U.S.C. 4713), if necessary and appropriate.

8. RESPONSIBILITIES.

a. Associate Administrator for Partnership and Acquisition Services.

(1) Ensure SRAs are completed for potential suppliers prior to the acquisition or extension of contracts awarded by the Office of Partnership and Acquisition Services for Critical Items.

(2) Deploys capabilities that vet or illuminate suppliers and contractual tools for mitigating those suppliers who represent an unacceptable level of risk to NSE supply chains.

(3) Ensures Procurement Contracting Officers review each M&O SCRM Plan annually.

(4) Initiates action(s) authorized by the EPA, if appropriate, after consultation with the NNSA Office of General Counsel (NA-GC), to address significant supply chain risks related to nuclear weapons and national security systems.

(5) Initiates action authorized by the FASCSA, if appropriate, after consultation with the NA-GC, to address significant supply chain risks related to information and communications technology (ICT) equipment and services.

b. Deputy Administrator for Defense Programs.

(1) Empowers the Supply Chain Risk Management Team (SCRMT) to collect, organize, evaluate, and share current supply chain risks and management practices across the NSE. Additionally, empowers the SCRMT to provide assistance, integration, and coordination to improve

support to the Nuclear Industrial Base (NIB). These efforts may also be accomplished via broader cross-DOE and U.S. Government enterprise collaboration venues.

(2) Empowers the NIB Monitoring Program to identify and share pertinent supply chain risk-related information and synchronize associated industrial base activities across the NSE and with other relevant stakeholders.

(3) Promotes SCRM awareness while developing and integrating SCRM principles and procedures within the Office of Defense Programs.

(4) Directs the Office of Defense Programs to identify, monitor, and assess the impact of potential disruptions related to NSE supply chains and mitigate risks within those relevant supply chains.

c. Deputy Administrator for Defense Nuclear Nonproliferation

(1) Promotes SCRM awareness while developing and integrating SCRM principles and procedures within the Office of Defense Nuclear Nonproliferation.

(2) Directs the Office of Defense Nuclear Nonproliferation to identify, monitor, and assess the impact of potential disruptions related to NSE supply chains and mitigate risks within those relevant supply chains.

d. Associate Administrator for Information Management and Chief Information Officer.

(1) Establishes, operates, and sustains an ICT SCRM or Cyber-SCRM (C-SCRM) capability or business process in compliance with directives and legislative mandates for the NSE.

(2) Collects and shares ICT/C-SCRM best practices and lessons learned with M&O Chief Information Officers, Chief Information Security Officers, and C-SCRM stakeholders on an annual basis.

(3) Provides mitigation strategies for NSE ICT and cybersecurity supply chain risks.

e. Associate Administrator for Infrastructure.

(1) Establishes, directs, and integrates SCRM principles and risk assessment methodologies into program management business processes.

(2) Ensures SRAs are completed for potential suppliers prior to the acquisition or extension of contracts awarded by the Office of Infrastructure for Critical Items. Not required for lower-tiered suppliers or contractors.

Collaborates with M&O contractors to enhance, share, and implement infrastructure SCRM best practices and lessons learned.

f. Field Office Managers.

(1) Ensure M&O contractors conduct SRAs for all procurements, and thereafter annually, for Critical Item subcontracts in accordance with the CRD.

(2) Ensure M&O contractors share the results of its SRAs and risk information with NSE laboratories, plants, sites, and programs via the Supply Chain Management Center (SCMC).

(3) Ensure the site Officially Designated Federal Security Authority, the Federal Classification Officer, and the Authorizing Official are provided access to the SRAs hosted by the SCMC.

(4) Ensure M&O contractors seek supply chain threat analysis and counterintelligence (CI) support from DOE's Office of Intelligence and Counterintelligence or their cognizant DOE CI Field Office.

g. Federal Program Managers and Federal Project Directors.

(1) Establish, direct, and integrate SCRM principles and risk assessment methodologies into program management business processes.

(2) Mitigate programmatic and technical supply chain risks through usage of the NIB Monitoring Program activities and information sharing among program offices.

(3) Provide supply chain risk information to the SCRMT on a quarterly basis for incorporation into the Enterprise Supply Chain Risk Framework.

(4) Collaborate with M&O contractors to define supply chain risk tolerance and threshold guidance to programs as well as laboratories, plants, and sites.

h. Field Office/Field Project Management Office Contracting Officers.

(1) Incorporate this NAP into the *List of Applicable Directives* identified in the *Laws, Regulations, and DOE Directives* clause of NNSA contracts and the M&O contracts within 3 months of the effective date of this NAP.

(2) Direct M&O contractors to share SRAs and risk information with NSE laboratories, plants, sites, and programs via the SCMC.

(3) Collaborate annually with other Field Offices' Contracting Officers to capture and implement best SCRM practices and lessons learned.

9. DEFINITIONS. See Attachment 2.

10. REFERENCES. See Attachment 3.

11. CONTACT. Questions concerning this NAP should be addressed to the Office of Partnership and Acquisition Services at (202) 586-4921.

BY ORDER OF THE ADMINISTRATOR:

Brandon M. Williams
Administrator

Attachments:
1. Contractor Requirements Document (CRD) – Marked separately as CUI//SP-PROCURE//FEDCON
2. Definitions
3. References

ATTACHMENT 1: CONTRACTOR REQUIREMENTS DOCUMENT
NAP 540.4, SUPPLY CHAIN RISK MANAGEMENT (SCRM)

Contact the National Nuclear Security Administration's Office of Partnership and Acquisition Services (NA-PAS-SCRM@nnsa.doe.gov) for this attachment as it is marked CUI//SP-PROCURE//FEDCON.

ATTACHMENT 2: DEFINITIONS

Note: This attachment applies to National Nuclear Security Administration (NNSA) contractor and Federal organizations.

a. Critical Item. Any of the following items or related services, to the extent that compromise of the item or service could cause substantial harm to national security, result in severe personal injuries or death, or otherwise significantly impede NNSA's missions:

(1) Component of a national security system (as defined in section 3552(b) of Title 44, United States Code [U.S.C.]).

(2) Component of a nuclear weapon.

(3) Item associated with the design, development, production, and maintenance of nuclear weapons.

(4) Item associated with the surveillance of the nuclear weapon stockpile.

(5) Item associated with the design and development of nonproliferation and counterproliferation programs and systems.

(6) To the extent that they receive, store, process, or transmit classified information, controlled unclassified information (CUI), export-controlled information, or will be present in Limited Areas or "higher":

(a) Information technology, as defined in section 11101 of Title 40 (40 U.S.C. 11101), including cloud computing services of all types.

(b) Telecommunications equipment or telecommunications service, as defined in section 3 of the *Communications Act* of 1934 (47 U.S.C. 153).

(c) Component related to the processing of information on a Federal or non-Federal information system, subject to the requirements of the CUI program; or

(d) hardware, systems, devices, software, or services that include embedded or incidental information technology.

(7) Any other item or service determined by the Contractor or NNSA to be integral to the Contractor's performance or NNSA's missions.

(8) Item, article, or technology that is export-controlled by 22 CFR 120-130, 10 CFR 110, 10 CFR 810, 15 CFR 730-774, and NAP 476.1.

b. Enterprise Supply Chain Risk Framework. NNSA quarterly reported risks from the Nuclear Security Enterprise that are gathered, scored, integrated, and categorized into a standardized risk register allowing quantification and analysis at an enterprise level for senior leader evaluation and consideration.

c. Nuclear Security Enterprise (NSE). Collective term for NNSA including Headquarters program and mission support offices, field offices, laboratories (Sandia National Laboratories, Los Alamos National Laboratory, and Lawrence Livermore National Laboratories), production plants (Y-12 National Security Complex, Pantex Plant, and Kansas City National Security Campus), and sites (the Savannah River Site, and the Nevada National Security Site).

d. Nuclear Industrial Base (NIB) Monitoring Program. An enterprise-wide effort led by the Office of Defense Programs' Office of Strategic Planning and Analysis that monitors the industrial base for the Nation's nuclear stockpile, which includes increasing connectivity and information sharing across the enterprise, proactively identifying gaps, and informing decisions to mitigate risks.

e. Supply Chain. A linked set of resources and processes between and among multiple levels of organizations, each of which is an acquirer that begins with the sourcing of products and services and extends through the product or service life cycle.

f. Supply Chain Management Center (SCMC). A strategic supply chain program operated by the management and operating (M&O) contractor responsible for the KCNSC dedicated to supporting the Department of Energy's Office of Environmental Management and NNSA prime contractors.

g. Supply Chain Risk (SCR). The potential for harm or compromise to the supply chain arises because of risk from suppliers, their supply chains, and their products or services. This includes the possibility that an individual may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a Critical Item to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of the Critical Item or systems in which it is a component.

h. Supply Chain Risk Management (SCRM). The process of proactively identifying supply chain vulnerabilities, threats, and potential disruptions and implementing mitigation strategies to ensure the security, integrity, and uninterrupted flow of materials, products, and services as risks are found or disruptions occur.sc

i. Supply Chain Risk Management Team (SCRMT). Chartered team directed by the Assistant Deputy Administrator for Systems Engineering and Integration; chartered members include NSE standing representatives and SCRM community stakeholders that meet monthly to capture, examine, organize, and prioritize enterprise-wide supply chain issues and risks.

ATTACHMENT 3: REFERENCES

Note: This attachment applies to National Nuclear Security Administration (NNSA) contractor and Federal organizations.

a. United States Code, Title 41, *Public Contracts and Property Management*, Subtitle D *Federal Acquisition Supply Chain Security*, Chapter 201 *Federal Acquisition Security Council*, Part 201-1, *General Regulations*, Subpart A – *General*; Subpart B – *Supply Chain Risk Information Sharing*; Subpart C – *Exclusion and Removal Orders*

b. 15 Code of Federal Regulations (CFR) 730-774 *Export Administration Regulation (EAR)* 22 CFR 120-130 *International Traffic in Arms Regulations (ITAR)*

c. 10 CFR 810 *Assistance to Foreign Atomic Energy Activities*

d. 10 CFR Part 110 *Export and Import of Nuclear Equipment and Material*

e. *Federal Acquisition Security Council Rule*, 86 FR 47581, effective 09-27-21

f. Federal Acquisition Regulation (FAR) Part 40, *Information Security and Supply Chain Security*

g. FAR Subpart 4.20, *Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab*

h. FAR Subpart 4.21, *Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment*

i. FAR Clause 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*

j. FAR Clause 52.204-23, *Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities*

k. FAR Clause 52.246-26, *Reporting Nonconforming Items*

l. Executive Order (EO)13873, *Securing the Information and Communications Technology and Services Supply Chain*, 05-17-19

m. EO 14017, *America's Supply Chains*, 02-24-21

n. National Institute of Standards and Technology Interagency or Internal Report (NISTIR) 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*, 02-11-21

o. NISTIR 8179, *Criticality Analysis Process Model: Helping Organizations Decide Which Assets Need to Be Secured First*, 04-11-18

p. Department of Energy (DOE) Order (O) 413.3, *Program and Project Management for the Acquisition of CapitalAssets*, current version

q. DOE O 414.1, *Quality Assurance*, current version

r. DOE O 452.4, *Security and Use Control of Nuclear Explosives and Nuclear Weapons*, current version

s. DOE O 470.4, *Safeguards and Security Program,* current version

t. DOE O 486.1, *Foreign Government Sponsored or Affiliated Activities*, current version

u. DOE Guide 413.3-7, *Risk Management Guide*, current version

v. DOE Guide 414.1-2, *Quality Assurance Program Guide*, current version

w. DOE Acquisition Letter No. AL-2021-06, *Chief Information Officer's Supply Chain Risk Management Program*, dated 09-01-21

x. NNSA Supplemental Directive 452.4-1, *Nuclear Enterprise Assurance (NEA)*, current version

y. NNSA Policy (NAP) 401.1, *Weapon Quality Policy*, current version

z. NAP 476.1, *Atomic Energy Act Control of Import and Export Activities,* current version