Nuclear Regulatory Commission
Office of the Chief Information Officer
Computer Security Process

Office Instruction:	**CSO-PROS-0013**
Office Instruction Title:	**Agency-Wide Supply Chain Risk Assessment Process**
Revision Number:	**1.1**
Effective Date:	**November 7, 2023**
Primary Contacts:	**Kathy Lyons-Burke** **Senior Level Advisor for Information Security**
Responsible Organization:	**OCIO/CSO**
Summary of Changes:	CSO-PROS-0013, "Agency-Wide Supply Chain Risk Assessment Process," defines the process that must be used to perform an agency-wide supply chain risk assessment.
ADAMS Accession No.:	ML23304A011

Agency Official	Approval Signature and Date
Jon Feibus Chief Information Security Officer (CISO) Office of the Chief Information Officer (OCIO)	Jonathan R. Feibus Digitally signed by Jonathan R. Feibus Date: 2023.11.02 16:24:00 -04'00'

Table of Contents

Computer Security Process
CSO-PROS-0013
Agency-Wide Supply Chain Risk Assessment Process

1 PURPOSE

CSO-PROS-0013 defines the process that must be used to perform an agency-wide supply chain risk assessment.

2 GENERAL REQUIREMENTS

This process must be performed annually and results must be stored in the Agencywide Documents and Management System (ADAMS) Agency-Wide Supply Chain Risk Assessments folder.

The Supply Chain Risk Management (SCRM) Working Group (WG) Co-Chairs performs an analysis of available information to determine the overall agency supply chain risk. The SCRM WG Co-Chairs use information supplied by sources across the agency to perform the analysis and document the risk assessment using CSO-TEMP-0013, "Agency-Wide Supply Chain Risk Assessment Template" (ML23208A020).

3 AGENCY-WIDE SUPPLY CHAIN RISK ASSESSMENT ROLES AND RESPONSIBILITIES

Table 1 identifies the roles and responsibilities associated with the agency-wide supply chain risk assessment.

Table 1: Agency-Wide Supply Chain Risk Assessment Roles and Responsibilities

Role	Responsibilities
Chief Information Security Officer (CISO)	• Reviews and either approves or rejects the agency-wide supply chain risk assessment. • Provides the Agency-Wide Supply Chain Risk Assessment (SCRA) to the Senior Agency Official for Supply Chain Risk Management (SAOSCRM) if the CISO cannot make a supply chain risk determination.
Information System Security Manager (ISSM) – formerly the Information System Security Officer (ISSO)	• Determines Recover: Recovery Planning Unacceptable Risk metric values
OCIO Cybersecurity Oversight Team (COT)	• Determines Identify: Risk Assessment presence metric values related to systems and the Federal Information Technology Acquisition Reform Act (FITARA). • Determines secure software attestation related metric values. • Determines counterfeit products related metric values.

Table 1: Agency-Wide Supply Chain Risk Assessment Roles and Responsibilities

Role	Responsibilities
	• Determines System Cybersecurity Assessments (SCA) related metric values. • Determines System Supply Chain Risk Assessments (SSCRA) related metric values. • Determines Protect: Identity Management and Access Control metric values. • Determines information technology staff and privacy staff training related metric values. • Determines Protect: Data Security metric values. • Determines Protect: Information Protection Processes and Procedures metric values. • Determines Protect: Maintenance metric values. • Determines Protect: Protective Technology metric values. • Determines Detect: Anomalies and Events metric values. • Determines Detect: Security Continuous Monitoring metric values. • Determines Detect: Detection process metric values. • Determines Respond: Response Planning metric values. • Determines Respond: Improvements metric values. • Determines Recover: Improvements system related metric values.
OCIO Security Operations Center (SOC)	• Determines Business Environment: Risk for Allegations/Investigations, Enforcement, Events Assessment, Inspection, and Licensing metric values. • Determines whether or not Cyber Threat Intelligence tools and services used to obtain, analyze, periodically report, and act on information regarding potential threats against the agency, federal government, and energy sector.
OCIO Service Fulfillment and Delivery Branch (SFDB)	• Determines Identify: Asset Management metric values.
Office of Administration (ADM) Acquisition, Policy, Planning, and Support Branch (APPSB)	• Determines Identify: Risk Assessment acquisition presence metric values. • Determines National Defense Authorization Act (NDAA) Section 889 certifications related metric values. • Determines acquisition staff training related metric values.
Office of Nuclear Security and Incident Response (NSIR)/ Division of Preparedness and Response (DPR)	• Determines Reecover: Recovery Planning Continuity of Operations Plan (COOP) specific metric values

Table 1: Agency-Wide Supply Chain Risk Assessment Roles and Responsibilities

Role	Responsibilities
SAOSCRM	• Reviews and either approves or rejects the agency-wide supply chain risk assessment.
SCRM WG Co-Chairs	• Performs overarching agency-wide supply chain risk assessment based upon inputs from responsible parties. • Determines Identify: Governance metric values. • Determines Identify: Business Environment presence metric values. • Determines Identify: Risk Management Strategy metric values. • Determines Identify: Supply Chain Risk Management metric values. • Determines Respond: Communications metric values. • Determines Respond: Analysis metric values. • Determines Respond: Mitigation metric values. • Determines Respond: Improvements metric values. • Determines Recover: Recovery Planning presence metric values. • Determines Recover: Communications metric values.

4 IDENTIFY FUNCTION

The Identify Function requires development of an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

4.1 Governance

Governance outcomes require that the policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform agency management of the associated cybersecurity risk.

The SCRM WG Co-Chairs review available information and determine the governance metrics. They then analyze the results and summarize the governance risk.

4.2 Asset Management

Asset Management outcomes require that the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

The SCRM WG Co-Chairs contact the OCIO SFDB and request the metric values for Asset Management. The SCRM WG Co-Chairs analyze the results and summarize the asset management risk.

4.3 Business Environment

Business Environment outcomes require that the organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

The SCRM WG Co-Chairs review available information and determine the business environment presence metrics.

The SCRM WG Co-Chairs contact the SOC and request the metric values for Allegations/Investigations, Enforcement, Events Assessment, Inspection, and Licensing risks.

The SCRM WG Co-Chairs analyze the results and summarize the business environment risk.

4.4 Risk Assessment

Risk Assessment outcomes require that the organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

The SCRM WG Co-Chairs contact the ADM APPSB and request the metric values for the acquisition process, TikTok, ByteDance, and NDAA Section 889 or the implementing Federal Acquisition Regulation (FAR) clauses.

The SCRM WG Co-Chairs contact the OCIO COT and request the metric values for the remaining risk assessment metrics.

The SCRM WG Co-Chairs analyze the results and summarize the risk assessment risk.

4.5 Risk Management Strategy

The SCRM WG Co-Chairs review available information and determine the governance metrics. They then analyze the results and summarize the risk management strategy risk.

4.6 Supply Chain Risk Management

The SCRM WG Co-Chairs review available information and determine the governance metrics. They then analyze the results and summarize the supply chain risk management risk.

5 PROTECT FUNCTION

The Protect Function requires development and implementation of appropriate safeguards to ensure delivery of critical services.

5.1 Identity Management and Access Control

Identity Management and Access Control outcomes require that access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

The SCRM WG Co-Chairs contact the OCIO COT and request the metric values for the Identity Management and Access Control metrics.

The SCRM WG Co-Chairs analyze the results and summarize the Identity Management and Access Control risk.

5.2 Awareness and Training

Awareness and Training outcomes require that the organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

The SCRM WG Co-Chairs contact the ADM APPSB and request the metric values for the acquisition staff training.

The SCRM WG Co-Chairs contact the OCIO COT and request the metric values for the remaining awareness and training metrics.

The SCRM WG Co-Chairs analyze the results and summarize the risk assessment risk.

5.3 Data Security

Data Security outcomes require that Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

The SCRM WG Co-Chairs contact the OCIO COT and request the metric values for the data security metrics.

The SCRM WG Co-Chairs analyze the results and summarize the risk assessment risk.

5.4 Information Protection Processes and Procedures

Information Protection Processes and Procedures outcomes require that security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

The SCRM WG Co-Chairs contact the OCIO COT and request the metric values for the Information Protection Processes and Procedures metrics.

The SCRM WG Co-Chairs analyze the results and summarize the Information Protection Processes and Procedures risk.

5.5 Maintenance

Maintenance outcomes require that maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

The SCRM WG Co-Chairs contact the OCIO COT and request the metric values for the Maintenance metrics.

The SCRM WG Co-Chairs analyze the results and summarize the Maintenance risk.

5.6 Protective Technology

Protective Technology outcomes require that technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

The SCRM WG Co-Chairs contact the OCIO COT and request the metric values for the Protective Technology metrics.

The SCRM WG Co-Chairs analyze the results and summarize the Protective Technology risk.

6 DETECT FUNCTION

The Detect Function requires development and implementation of appropriate activities to identify the occurrence of a cybersecurity event.

6.1 Anomalies and Events

Anomalies and Events outcomes require that anomalous activity is detected and the potential impact of events is understood.

The SCRM WG Co-Chairs contact the OCIO COT and request the metric values for the Anomalies and Events metrics.

The SCRM WG Co-Chairs analyze the results and summarize the Anomalies and Events risk.

6.2 Security Continuous Monitoring

Security Continuous Monitoring outcomes require that the information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

The SCRM WG Co-Chairs contact the OCIO COT and request the metric values for the Security Continuous Monitoring metrics.

The SCRM WG Co-Chairs analyze the results and summarize the Security Continuous Monitoring risk.

6.3 Detection Process

Detection Process outcomes require that detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

The SCRM WG Co-Chairs contact the OCIO COT and request the metric values for the Detection Process metrics.

The SCRM WG Co-Chairs analyze the results and summarize the Detection Process risk.

7 RESPOND FUNCTION

The Respond Function requires development and implementation of appropriate activities to address a detected cybersecurity incident.

7.1 Response Planning

Response Planning outcomes require that response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

The SCRM WG Co-Chairs contact the OCIO COT and request the metric values for the Response Planning metrics.

The SCRM WG Co-Chairs analyze the results and summarize the Response Planning risk.

7.2 Communications

Communications outcomes require that response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).

The SCRM WG Co-Chairs review available information and determine the Communications metrics. They then analyze the results and summarize the supply chain risk management risk.

7.3 Analysis

Analysis outcomes require that analysis is conducted to ensure effective response and to support recovery activities.

The SCRM WG Co-Chairs review available information and determine the Analysis metrics. They then analyze the results and summarize the supply chain risk management risk.

7.4 Mitigation

Mitigation outcomes require that activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

The SCRM WG Co-Chairs review available information and determine the Mitigation metrics. They then analyze the results and summarize the supply chain risk management risk.

7.5 Improvements

Improvements outcomes require that organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

The SCRM WG Co-Chairs review available information and determine the Improvements metrics. They then analyze the results and summarize the supply chain risk management risk.

8 RECOVER FUNCTION

The Recover Function requires development and implementation of appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

8.1 Recovery Planning

Recovery Planning outcomes require that recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

The SCRM WG Co-Chairs contact the ISSMs and request the metric values for the Recovery Planning Unacceptable Risk metrics.

The SCRM WG Co-Chairs review available information and determine the Recovery Planning presence metrics. They then analyze the results and summarize the supply chain risk management risk.

8.2 Improvements

Improvements outcomes require that recovery planning and processes are improved by incorporating lessons learned into future activities.

The SCRM WG Co-Chairs review available information and determine the Improvements metrics. They then analyze the results and summarize the supply chain risk management risk.

8.3 Communications

Communications outcomes require that restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers (ISPs), owners of attacking systems, victims, other Computer Security Incident Response Teams [CSIRTs], and vendors).

The SCRM WG Co-Chairs review available information and determine the Communications metrics. They then analyze the results and summarize the supply chain risk management risk.

9 ILLUMINATION INFORMATION

An Illumination is a product produced by Exiger Subject Matter Experts that provides a macro/large-scale identification, assessment, and visualization of a program, product, or sectoral supply chain.

The SCRM WG Co-Chairs review available illumination information and create a subsection for each illumination performed since the last agency-wide SCRA that provides an overall description of the purpose of the illumination, high-level findings, and an analysis of the resulting risk to the NRC.

10 SUPPLY CHAIN RISK SUMMARY

The SCRM WG Co-Chairs summarize all of the SCRM risk findings and review available illumination information and create a subsection for each illumination performed since the last agency-wide SCRA that provides an overall description of the purpose of the illumination, high-level findings, and an analysis of the resulting risk to the NRC. The SCRM WG Co-Chairs then identify the current SCRM risk to the NRC.

11 ACTIONS REQUIRED

The SCRM WG Co-Chairs all actions that are required as a result of the SCRM risk assessment.

APPENDIX A ACRONYMS

ADAMS	Agencywide Documents and Management System
ADM	Office of Administration
APPSB	Acquisition, Policy, Planning, and Support Branch
CISO	Chief Information Security Officer
COOP	Continuity of Operations Plan
COT	OCIO Cybersecurity Oversight Team
CSIRT	Computer Security Incident Response Team
CSO	Computer Security Organization
DCISO	Deputy Chief Information Security Officer
DPR	NSIR Division of Preparedness and Response
FITARA	Federal Information Technology Acquisition Reform Act
FY	Fiscal Year
ICT	Information and Communications Technology
ISP	Internet Service Providers
ISSM	Information System Security Manager
ISSO	Information System Security Officer
MD	Management Directive
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSIR	Office of Nuclear Security and Incident Response
OCIO	Office of the Chief Information Officer
SAOSCRM	Senior Agency Official for Supply Chain Risk Management
SCA	System Cybersecurity Assessments
SCRA	Supply Chain Risk Assessment

SCRM	Supply Chain Risk Management
SFDB	OCIO Service Fulfillment and Delivery Branch
SOC	OCIO Security Operations Center
SP	Special Publication
SSCRA	System Supply Chain Risk Assessment
WG	Working Group

APPENDIX B REFERENCES

LAWS AND EXECUTIVE ORDERS

[CLINGER] Clinger-Cohen Act (P.L. 104-106), February 1996, https://www.govinfo.gov/app/details/PLAW-104publ106

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

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

[EO 14028] EO 14028, Improving the Nation’s Cybersecurity

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

[FISMA] Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.govinfo.gov/app/details/PLAW-113publ283

[FITARA] Federal Information Technology Acquisition Reform Act (P.L. 115-88), November 2017. https://www.govinfo.gov/app/details/PLAW-115publ88

[NDAA-889] FY 2019 National Defense Authorization Act Section 889

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

POLICIES, REGULATIONS, DIRECTIVES, AND INSTRUCTIONS

[OMB A-123] Office of Management and Budget Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, July 2016. https://www.whitehouse.gov/omb/information-for-agencies/circulars/

[OMB A-130] Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource, July 2016. https://www.whitehouse.gov/omb/information-for-agencies/circulars/

[OMB-M-17-09] M-17-09, “Management of Federal High Value Assets”

[OMB-M-19-03] M-19-03, “Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program”

[OMB-M-21-30] M-21-30, “Protecting Critical Software Through Enhanced Security Measures”

[OMB-M-22-18] M-22-18, “Enhancing the Security of the Software Supply Chain through Secure Software Development Practices”

[OMB-M-23-13] M-23-13, “No TikTok on Government Devices” Implementation Guidance”

[OMB-M-23-16] M-23-16, “Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices”

STANDARDS, GUIDELINES, AND REPORTS

[SP 800-30]	NIST SP 800-30, "Guide for Conducting Risk Assessments", Revision 1, September 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
[SP 800-37]	NIST SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2, December 2019. https://doi.org/10.6028/NIST.SP.800-37r2
[SP 800-39]	NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011. https://doi.org/10.6028/NIST.SP.800-39
[SP 800-53]	NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations, September 2020. https://doi.org/10.6028/NIST.SP.800-53r5
[SP 800-161]	NIST SP 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, May 2022. https://doi.org/10.6028/NIST.SP.800-161r1

NRC DOCUMENTS

[CSO-PLAN-0100]	CSO-PLAN-0100, "Enterprise Risk Management Program Plan"
[ICT Risk Tolerance]	Information and Communications Technology Risk Tolerance, Revision 1.0, ML21096A110
[MD 12.0]	MD 12.0, "Glossary of Security Terms"
[MD 12.5]	MD 12.5, "NRC Cybersecurity Program"
[NRC COOP]	NRC Continuity of Operations Plan, ML14024A688
[MRF-BIA]	NRC MEF Business Impact Analysis (BIA) Worksheet, ML18318A007
[IT-Sys-Crit]	NRC IT System Criticality Tool, ML16064A419
[NRC ISA]	NRC Information Security Architecture, Version 1.0, July 2, 2021
[NRC SP]	NRC Strategic Plan Fiscal Years 2022-2026, NUREG-1614, Vol. 8
[Risk strategy]	NRC Risk Management Strategy, Revision 1.0, ML20266G443
[SCRM Strategy]	NRC Supply Chain Risk Management Strategy, Revision 1.0, September 2020, ML20310A085

APPENDIX C GLOSSARY

Exiger	Supply chain risk service that uses an AI-powered Platform to drive transformational change in how entities are vetted at an unprecedented scale. DDIQ identifies, validates and analyzes global risk indicators by aggregating open source information, performing entity disambiguation, assessing and continuously monitoring ongoing risk to the companies and suppliers within the relevant supply chain network.
ICT	Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks). Source(s): CNSSI 4009-2015 from DoDI 5200.44
ICT Products	Information and communication technology hardware, software, or services.
Illumination	Illumination: Macro/large-scale identification, assessment, and visualization of a program, product, or sectoral supply chain. Utilizes both DDIQ and Exiger Subject Matter Experts to uncover complex risk trends across hundreds or thousands of relevant entities, vendors, contracts, or other links in the targeted supply chain.
Non-Tier 1 HVAs	Represent systems of significant impact to both the agency and the nation.
SCRA	An NRC created supply chain risk assessment document that identifies an NRC SCR acceptance determination and the rationale supporting the determination.
Tier 1 HVAs	Represent systems of critical impact to both the agency and the nation.

CSO-PROS-0013 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
23-Oct-23	1.0	Initial release	Monthly Office Meetings.	None needed.