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

Office Instruction:	**CSO-PROS-0008**
Office Instruction Title:	**Process to Assess, Respond to, and Monitor ICT Supply Chain Risks**
Revision Number:	**1.0**
Effective Date:	**01-Aug-23**
Primary Contacts:	**Kathy Lyons-Burke** **Senior Level Advisor for Information Security**
Responsible Organization:	**OCIO/CSO**
Summary of Changes:	CSO-PROS-0008, “Process to Assess, Respond to, and Monitor ICT Supply Chain Risks,” defines the process that must be used to determine the supply chain risk associated with an Information and Communications Technology (ICT) product or service, perform appropriate responsive actions, and monitor the risk over time.
ADAMS Accession No.:	ML21287A091

Agency Official	**Approval Signature and Date**
Garo Nalabandian Chief Information Security Officer (CISO) Office of the Chief Information Officer (OCIO)	Garo Nalabandian Digitally signed by Garo Nalabandian Date: 2023.07.26 10:11:41 -04'00'

Table of Contents

Computer Security Process
CSO-PROS-0008
Process to Assess, Respond to, and Monitor ICT Supply Chain Risks

1 PURPOSE

CSO-PROS-0008 defines the process that must be used to determine the supply chain risk associated with an Information and Communications Technology (ICT) product or service, perform appropriate responsive actions, and monitor the risk over time.

This process is only used initially for products NRC is currently using. The process will be applied to items planned to be acquired, for cost or with no cost, as criteria associated with selections after the process has been refined based upon lessons learned from use. Any text that applies only to new acquisitions or to requirements that are not fully in place yet is in red to notify the reader that those items are not yet effective.

2 GENERAL REQUIREMENTS

This process must be performed for each ICT product and service that NRC uses or intends to use and results must be stored in the Supply Chain Risk Management Working Group SharePoint supply chain risk repository associated with the product or service and in the ADAMS folder dedicated to those results. Three components are required for each purchase:

- A National Defense Authorization Act (NDAA) Section 889 Certification
- A Secure Software Attestation (for software acquisitions)
- A Supply Chain Risk Assessment (SCRA)

3 SUPPLY CHAIN RISK ASSESSMENT, RESPONSE, AND MONITORING ROLES AND RESPONSIBILITIES

Table 1 provides the roles and responsibilities associated with supply chain risk assessment, response, and monitoring. Staff that hold the roles below are identified on the Computer Security Organization SharePoint site, OCIO GEMS Cyber Security Branch SharePoint site, and Nuclepedia page for NRC's Supply Chain Risk Management.

Table 1: Supply Chain Risk Assessment, Response, and Monitoring Roles and Responsibilities

Role	Responsibilities
Chief Information Security Officer (CISO)	• Provides Risk Determination to Cybersecurity SC Assessor if the SC Assessor could not make the determination or if the CISO disagrees with the SC Assessor determination. • Provides the SCRA to the Senior Agency Official for Supply Chain Risk Management (SAOSCRM) if the CISO cannot make a supply chain risk determination. • Reviews and either approves or rejects the Cybersecurity SC Assessor supply chain risk determination.

Table 1: Supply Chain Risk Assessment, Response, and Monitoring Roles and Responsibilities

Role	Responsibilities
	• Provides the System Supply Chain Risk Assessment (SSCRA) to the Senior Agency Official for Supply Chain Risk Management (SAOSCRM) if the CISO cannot make a supply chain risk determination. • Reviews and either approves or rejects the ISSM plan to address SSCRA identified risks. • Ensures product removal plans appropriately address NRC supply chain risk and ensures the product removal is completed. • Notifies the SAOSCRM as soon as possible when the supply chain risk associated with a product in use is unacceptable. • Obtains any needed SCRA service illuminations. • Obtains any needed Supply Chain Risk Assessment (SCRA) Enhanced Due Dilligence (EDD) reports.
Contracting Officer (CO)	• Ensures an NRC acceptable attestation of secure software development practices is obtained before a vendor is awarded a contract. • Verifies NDAA Section 889 Compliance for each contractor before they are awarded a contract. • Completes CO Vendor SCR using the SCRA Template for Contracting Officers. • Ensures that an SCRA is performed and a risk determination is made for each contractor and product or service before contract award. • Obtains Vendor provided Supply Chain Risk (SCR) information as submitted using the SCRA Template for Offerors.
Contracting Officer's Representative (COR)	• Obtains an attestation of secure software development practices from the software producer, stores the information in the Secure Software Attestations Repository, and obtains Cybersecurity SC Assessor approval prior to acquiring a product. • Ensures that an SCRA is performed and a risk determination is made for each contractor and product or service before contract award.
Cybersecurity Secure Software Attestation Reviewer (CSSAR)	• Reviews software producer secure software attestations and makes a determination on acceptability of software use for low, moderate, and high assurance functions. • Stores the determination information in the Secure Software Attestations Repository.
Information System Security Manager (ISSM) – formerly the Information System Security Officer (ISSO)	• Performs an SSCRA at the required frequency. • Provides the SSCRA to the CISO for concurrence and signature. • Stores the signed SSCRA with the other system artifacts.

Table 1: Supply Chain Risk Assessment, Response, and Monitoring Roles and Responsibilities

Role	Responsibilities
	• Ensures that a supply chain risk assessment is performed and an acceptable level of risk is in place prior to any acquisitions. If the acquisition is a contract acquisition, the ISSM notifies the COR, CO, and contract specialist of the supply chain risk acceptance or rejection determination as soon as possible. • Monitors the supply chain risk associated with vendors and products used by their system. This includes monitoring the CISA site for notifications about vendors and products that reflect on supply chain risk. • Develops a plan to address SSCRA identified risks and provides the plan to the CISO for approval. • Develops product removal plans in coordination with the project manager, obtains CISO approval of the plan, and ensures the product removal is completed.
OCIO Cybersecurity Intake Lead	• For software purchases, ensures an acceptable attestation of secure software development is available in the Secure Software Attestations Repository. • Develops the required NDAA Section 889 certification for those acquisitions that do not have an NDAA Section 889 certification using CSO-PROS-0011, "Supply Chain Evaluation Process for NDAA Section 889 when Certification not Available" and records the certification in the NDAA Section 889 repository. • Ensures to a reasonable degree that the requested product does not violate NDAA Section 889. • Ensures that the supply chain risk assessment for the purchase request represents an acceptable level of risk.
OCIO Cybersecurity Oversight Team Assigned Assessor (referred to in text as Cybersecurity SC Assessor)	• For products/services where an NDAA Section 889 certification is not available, uses CSO-PROS-0011, "Supply Chain Evaluation Process for NDAA Section 889 when Certification not Available" to evaluate the NDAA Section 889 applicability to the product/service. • Performs an NDAA Section 889 relevant investigation for ICT products where an NDAA Section 889 certification/representation is not available. • Resonsible for using the Exiger service to create full profiles for companies that product or sell ICT products and services. • Documents SCRA and risk determination in CSO-TEMP-0008, "ICT Supply Chain Risk Assessment Template." • Notifies requester and ISSM if more information is needed to make a risk determination. • Uses CSO_GUID-7001, "Guide to Generating an Exiger Profile" to generate the Exiger profiles for use in developing an SCRA. • Uses CSO-PROS-0007, "Process to Use SCR Investigation Service to Determine ICT Supply Chain Risk Associated with an Offeror" to determine if the supply chain risk should be accepted or rejected. • Provides SCRA document with an initial risk determination to CISO.

Table 1: Supply Chain Risk Assessment, Response, and Monitoring Roles and Responsibilities

Role	Responsibilities
	• Provides final Risk Determination to Requester and Supply Chain Product Risk Technical Review Lead. • Updates the EDD-List list with information for each Exiger Deep Dive performed. • Updates the Illumination_Index list with information for each illumination performed. • Updates the SCRA_Index list with information from the risk assessment. • Updates the SCRA_Actions list with all the actions required by the SCRA.
Cybersecurity Secure Software Reviewer (CSSR)	• Performs a review of the attestation to determine if the attestation is sufficient for the software purpose. • Notifies the contracting officer, purchase card holder, or No-Cost SCR Lead of the determination as to acceptability for the software's identified purpose and stores the determination information in the Secure Software Attestations Repository.
OCIO Cybersecurity Oversight Team Lead	• Assigns supply chain risk assessments to a Cybersecurity SC Assessor to perform the supply chain risk assessment. • Assigns the attestation review to a member of the team that serves as the CSSAR.
OCIO No Cost SCRM HW/SW Lead (No-Cost SCR Lead)	• For all requests to acquire no cost ICT products: – Obtains an attestation of secure software development practices from the software producer, stores the information in the Secure Software Attestations Repository, and obtains Cybersecurity SC Assessor approval prior to acquiring a product. – Determines if a less than 1 year old NDAA Section 889 certification is available in the NDAA Section 889 repository. If so, the requirement is met. – If a valid certification is not available in the repository, obtains NDAA Section 889 certification for all requests to acquire no cost ICT products and records the certification in the NDAA Section 889 repository. – Refers request to the OCIO Cybersecurity Intake Lead when an NDAA Section 889 certification/representation is not available.
OCIO Purchase Card SCRM HW/SW Lead (Purchase Card SCR Lead)	• For all requests to acquire ICT products via a purchase card: – Determines if a less than 1 year old NDAA Section 889 certification is available in the NDAA Section 889 repository. If so, the requirement is met. – If a valid certification is not available in the repository, obtains NDAA Section 889 certification for all requests to acquire no cost ICT products and records the certification in the NDAA Section 889 repository. – Refers request to the OCIO Cybersecurity Intake Lead when an NDAA Section 889 certification/representation is not available.

Table 1: Supply Chain Risk Assessment, Response, and Monitoring Roles and Responsibilities

Role	Responsibilities
	– Obtains an attestation of secure software development practices from the software producer, stores the information in the Secure Software Attestations Repository, and obtains Cybersecurity SC Assessor approval prior to acquiring a product.
Project Manager	• Assists the ISSM in developing product removal plans, obtaining CISO approval of the plan, and ensuring the product removal is completed.
Purchase card holders	• Obtains an attestation of secure software development practices from the software producer, stores the information in the Secure Software Attestations Repository, and obtains Cybersecurity SC Assessor approval prior to acquiring a product. • Notifies the OCIO Cybersecurity Intake Lead if the NDAA Section 889 certification is not available. • Records the NDAA section 889 certification in the NDAA Section 889 repository. • Requests NDAA Section 889 certification from the vendor if it is not already available in the NDAA Section 889 repository or if the one available is older than 1 year. • Verifies NDAA Section 889 Compliance for each purchase before completing purchase.
Senior Agency Official for Supply Chain Risk Management (SAOSCRM)	• May approve a request for an EDD report or an illumination. • Makes the determination of whether or not to accept or reject the supply chain risk associated with an offeror when the criteria defined in CSO-PROS-0007, “Process to Use SCR Investigation Service to Determine ICT Supply Chain Risk Associated with an Offeror” is inconclusive and the CISO cannot make the determination. • Notifies the CISO of the risk determination and signs the SCRA.
Supply Chain Product Risk Technical Review Lead (SCPRTRL)	• Obtains SCRAs for products currently deployed at NRC in accordance with the Appendix B, Criteria for Prioritizing Supply Chain Risk Assessments for ICT Products and Services. • Maintains SCRA information and risk acceptance or rejection information for all ICT products and services.

4 NDAA SECTION 889 DETERMINATION

The fiscal year (FY) 2019 NDAA prohibits agencies from purchasing telecommunications equipment and services produced or provided by specific entities, including all subsidiaries or affiliates and prohibits the government from doing business with entities that use end products produced by these companies. It also covers the use of any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Please refer to the acquisitions NRC’s Enterprise Acquisition Toolset (NEAT) website for instructions and information regarding NDAA Section 889 compliance.

If an ICT product or service is not NDAA Section 889 compliant, NRC must **not** acquire the product or service and must stop using any products or services already in use as soon as possible.

4.1 Contract Acquisitions

All contractors doing or seeking to do business with the NRC must provide a statement of NDAA Section 889 compliance. These compliance statements are available via the System for Award Management (SAM) website.

For these acquisitions, the CO searches the SAM database for the NDAA Section 889 certification for the vendor. If the certification is found, the COR documents the results using the Section 889 Compliance Template [889-Template]. If the certification is not found, the CO requests the certification from the provider and may not award a contract until the certification is provided.

4.2 Purchase Card Acquisitions

Purchase card holders must obtain an NDAA Section 889 certification for all purchase card requests. The purchase card holder first checks the SAM website to determine if the vendor's current (less than 1 year old) certification is there. If so, the NDAA Section 889 certification requirement is met. If not, the purchase card holder checks the NRC NDAA Section 889 Repository to see if a current (less than 1 year old) certification is in the repository. If so, the NDAA Section 889 certification requirement is met.

If a current, valid NDAA Section 889 certification is not available, the purchase card holder uses the Section 889 Certification Email Template for Purchase Card Holders [889-Email-Purchase-Card] for all purchase card purchases to obtain the required certification from the vendor. Once the certification is obtained, the purchase card holder records the certification in the NDAA Section 889 Repository, and the NDAA Section 889 certification requirement is met..

If the purchase card holder cannot obtain an NDAA Section 889 certification from the vendor, the purchase card holder notifies the OCIO Cybersecurity Intake Lead that a purchase is requested, and they were not able to obtain a certification from the vendor.

The purchase card holder must wait for the OCIO Cybersecurity Intake Lead to provide an NDAA Section 889 risk determination for the vendor. If the risk is determined to be acceptable, the purchase card holder may continue with the purchase.

4.3 No Cost Acquisitions

The No-Cost SCR Lead must obtain an NDAA Section 889 certification for all no cost acquisitions. The No-Cost SCR Lead first checks the System for Award Management (SAM) website to determine if the provider's current (less than 1 year old) certification is there. If so, the NDAA Section 889 certification requirement is met. If not, the No-Cost SCR Lead checks the NDAA Section 889 Repository to see if a current (less than 1 year old) certification is in the repository. If so, the NDAA Section 889 certification requirement is met.

If a current, valid NDAA Section 889 certification is not available, the No-Cost SCR Lead uses the Section 889 Certification Email Template for Purchase Card Holders [889-Email-Purchase-Card] for all no-cost purchases to obtain the required certification from the provider. Once the

certification is obtained, the No-Cost SCR Lead records the certification in the NDAA Section 889 Repository, and the NDAA Section 889 certification requirement is met.

If the No-Cost SCR Lead cannot obtain an NDAA Section 889 certification from the provider, the No-Cost SCR Lead notifies the OCIO Cybersecurity Intake Lead that a purchase is requested, and they were not able to obtain a certification from the vendor.

4.4 Cybersecurity Intake

When the OCIO Cybersecurity Intake Lead receives a notification from a purchase card holder or No-Cost SCR Lead that an NDAA Section 889 certification is not available, the OCIO Cybersecurity Intake Lead uses CSO-PROS-0011, “Supply Chain Evaluation Process for NDAA Section 889 when Certification not Available” to evaluate NDAA section 889 issues. The OCIO Cybersecurity Intake Lead provides a documented evaluation to the purchase card holder or No-Cost SCR Lead, and places the evaluation into the NDAA Section 889 Repository.

5 SECURE SOFTWARE ATTESTATIONS

OMB memorandum M-22-18, "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices" requires federal agencies to obtain and store software producer's self-attestation of secure software development practices. NRC must retain the self-attestation document unless the software producer posts it publicly and provides a link to the posting. The documented attestation must have a filename in the format SWProducerName_Attestation_YYYYMMDD where SWProducerName is the software producer’s name, YYYY is the year the attestation was signed, MM is the the attestation was signed, and DD is the day the the attestation was signed.

The Secure Software Attestations Repository includes a list entry for each vendor for which an attestation is available. The list contains a link to the attestation, which is to the SharePoint document library file in the repository or to the location where the producer provides a public self-attestation.

If a software vendor does not have an acceptable secure software attestation, NRC must **not** acquire the product or service and must stop using any products or services already in use as soon as possible.

The contracting officer, purchase card holder, or No-Cost SCR Lead obtains an attestation of secure software development practices from the software producer and updates the Secure Software Attestations Repository. If the attestation is a link to a public site, the index is updated with the relevant producer information and the link to the attestation. If the attestation is a provided document, the document is stored in the repository document library and the index is updated with the producer information and a link to the document in the document library.

Once the attestation is available, the contracting officer, purchase card holder, or No-Cost SCR Lead notifies the Cybersecurity Oversight Team Lead of the software purpose and the availability of the attestation. The Cybersecurity Oversight Team Lead assigns the attestation review to a member of the team that serves as the CSSAR. The CSSAR performs a review of the attestation to determine if the attestation is sufficient for the software purpose. The CSSAR notifies the contracting officer, purchase card holder, or No-Cost SCR Lead of the determination as to acceptability for the software’s identified purpose and stores the determination information in the Secure Software Attestations Repository.

6 VENDOR SUPPLY CHAIN RISK ASSESSMENT

All acquisitions that are not purchase card acquisitions or no-cost acquisitions must require the offeror to complete a supply chain risk vendor form using the Supply Chain Risk Assessment (SCRA) Template for Offerors [SCR_Offeror_Info]. The acquisition contracting officer uses the submitted information to complete the Supply Chain Risk Assessment (SCRA) Template for Contracting Officers [CO_SCR_Vendor_Rev].

The OCIO Cybersecurity Oversight Team Lead searches the SCRA Index to determine is a current SCRA exists. The default currency of the SCRAs is 7 years. An SCRA may require a new assessment sooner. If there is not a current SCRA, the OCIO Cybersecurity Oversight Team Lead assigns a member of the team to be the Cybersecurity SC Assessor. The Cybersecurity SC Assessor may use contractor support to complete the SCRA, but remains responsible for the risk determination and communication with others related to the SCRA.

The individual responsible for acquisition of the product or service must ensure that a supply chain risk acceptance is in place prior to acquiring the product or service.

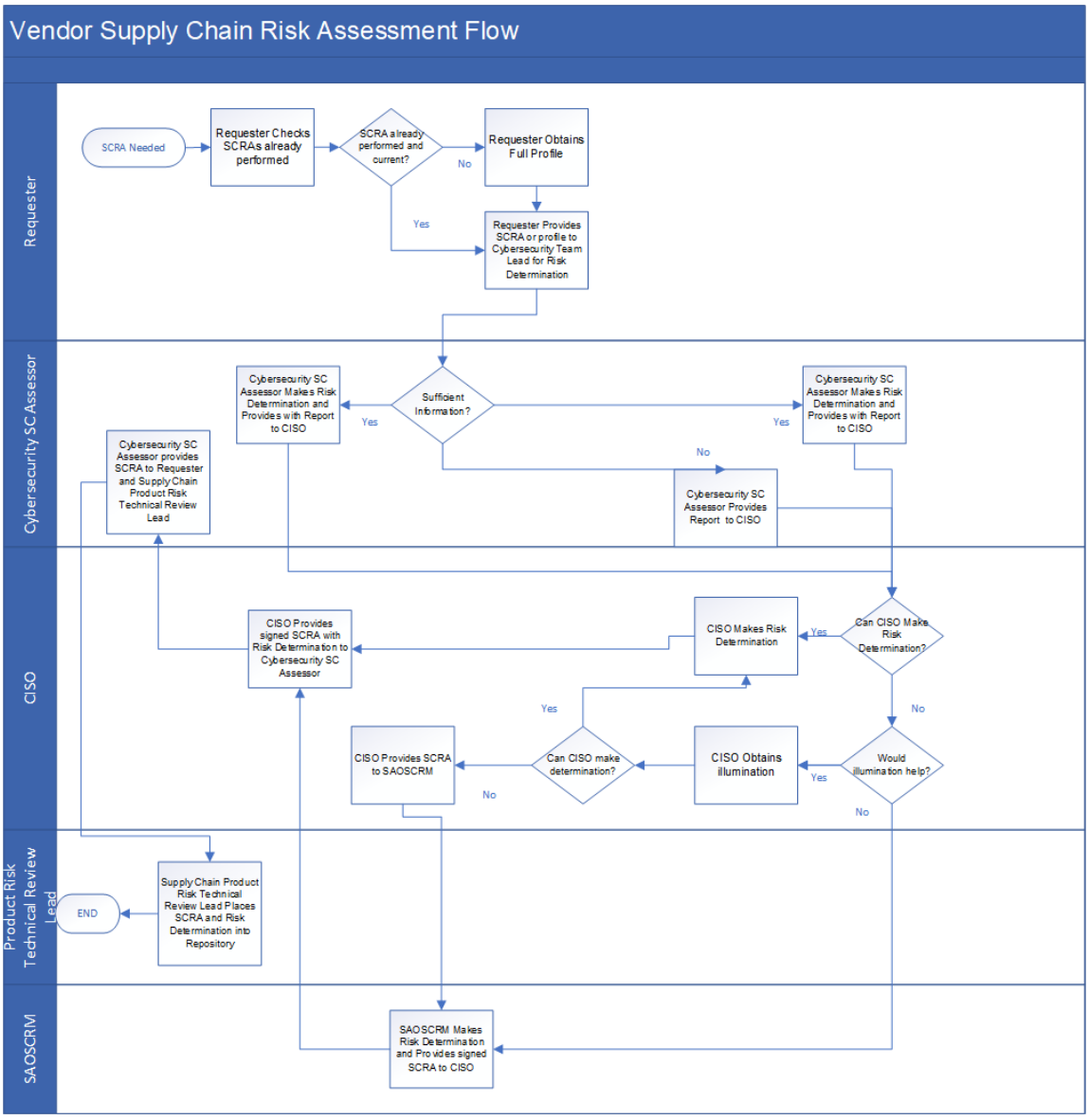

Figure 1: Vendor Supply Chain Risk Assessment Flow

6.1 Products in Use

The Supply Chain Product Risk Technical Review Lead must ensure an SCRA is performed for all products currently being used by the NRC. Those risk assessments must be prioritized using the Criteria for Prioritizing Supply Chain Risk Assessments for ICT Products and Services. The Supply Chain Product Risk Technical Review Lead provides each SCRA to the Cybersecurity Oversight Team Lead for a supply chain risk acceptance or rejection determination.

6.2 Acquisitions

An acquisition may only occur with an acceptable risk determination is made based upon an SCRA. The ISSM Leads acquisition efforts to ensure the supply chain risk is acceptable prior to any acquisition.

The CO and COR must work with the ISSM to ensure an SCRA is performed for all products prior to an acquisition selection. The ISSM provides each SCRA as well as the vendor provided SCR information to the Cybersecurity SC Assessor for a supply chain risk acceptance or rejection determination. If the acquisition is a contract acquisition, the ISSM notifies the COR, CO, and contract specialist of the supply chain risk acceptance or rejection determination as soon as possible.

The ISSM provides each SCRA and acceptance or rejection determination to the Supply Chain Product Risk Technical Review Lead, and the Supply Chain Product Risk Technical Review Lead must ensure that the SCRA and risk acceptance or rejection determination are stored in the supply chain risk information repository and associated with the subject of the risk assessment.

6.3 Requesting an Exiger SCR Profile

NRC currently has a supply chain risk assessment service that should be used to perform a supply chain risk assessment for a specific acquisition. That service should be employed for all acquisitions. Bulk uploads of vendors can be accommodated by the service, if needed.

Access to the SCRA service tool and reports should be restricted to NRC staff and to contractors that have signed a non-disclosure agreement. All requests for SCRA service must be made through the SCRA service COR. **All reports must be labeled as proprietary information.** The Cybersecurity SC Assessor uses CSO_GUID-7001, “Guide to Generating an Exiger Profile” to generate the Exiger profiles for use in developing an SCRA.

The Cybersecurity SC Assessor uses the following order to obtain a supply chain risk assessment determination for an ICT product or service:

1. Check supply chain risk determinations already performed, their applicability to the acquisition being evaluated, and the currency of the determination. These may have been performed by another agency to which NRC has been granted access.
2. First supply chain risk assessments for a contractor/vendor/product should use the SCRA service full profile. If there aren’t any areas that need further elaboration, this search should be sufficient.
3. If an SCRA service full profile report is inconclusive, an EDD report may be appropriate. Any requests for EDD reports must be approved by the CISO or SAOSCRM.
4. If an SCRA service EDD report is inconclusive, an illumination may be appropriate. Any requests for illuminations must be approved by the CISO or SAOSCRM.

6.4 Developing an SCRA

The Cybersecurity SC Assessor examines the NDAA Section 889 certification documentation received. If the certification provides the necessary information to believe the provider is NDAA

Section 889 compliant, the Cybersecurity SC Assessor approves the NDAA Section 889 compliance aspect of the acquisition.

If the product includes software, the Cybersecurity SC Assessor examines the secure software attestation determination for the software purpose. If the determination is that the attestation is acceptable for the software purpose, the Cybersecurity SC Assessor approves the attestation aspect of the acquisition.

The Cybersecurity SC Assessor uses CSO-PROS-0007, “Process to Use SCR Investigation Service to Determine ICT Supply Chain Risk Associated with an Offeror” to determine if the supply chain risk should be accepted or rejected and CSO-TEMP-0008, “ICT Supply Chain Risk Assessment Template” to document the risk assessment and risk determination. If more information is needed to make a risk determination, notifies the requester and ISSM. If the Cybersecurity SC Assessor feels that additional analyst detail is needed to make a risk determination, the Cybersecurity SC Assessor requests approval to request an EDD from the Exiger service.

The Cybersecurity SC Assessor must place SCRAs into ADAMS in accordance with CSO-PROS-0007as the basis for the SCRM decision but labeled as proprietary information and access appropriately restricted.

The Cybersecurity SC Assessor must update the SCRA_Index with information from the risk assessment and the SCRA_Actions list with all the actions required by the SCRA.

For each EDD requested, the Cybersecurity SC Assessor must update the EDD-List list with information for each Exiger Deep Dive performed.

For each Illumination requested, the Cybersecurity SC Assessor must update the Illumination Index list with information for each illumination performed.

7 SYSTEM SUPPLY CHAIN RISK ASSESSMENT

The ISSM obtains an independent system risk assessment of supply chain related information and artifacts that assesses supply chain risks associated with systems, system components, and system services initially and when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain. This risk assessment is called an SSCRA. This assessment must be performed every 5 years or upon a major system change.

8 SUPPLY CHAIN RISK DETERMINATION

A supply chain risk determination must be made for products and services being used or that may be used by NRC.

8.1 System Supply Chain Risk Determination

The ISSM develops an SSCRA with a supply chain risk determination and provides it to the CISO for concurrence. The CISO reviews the determination. If the CISO does not agree with the determination, the CISO modifies the determination or requests additional information to make a risk determination. If the results in the determination are inconclusive, the CISO provides the SCRA to the SAOSCRM to make an acceptance or rejection determination. Once

the CISO has an acceptable determination, the CISO provides the determination to the ISSM and signs the SSCRA. The ISSM must develop a plan to address identified risks, and the CISO must approve the plan.

8.2 Vendor Supply Chain Risk Determination

The Cybersecurity SC Assessor provides the SCRA and supply chain risk determination to the CISO. The CISO reviews the determination. If the CISO does not agree with the determination, the CISO modifies the determination or requests additional information to make a risk determination and signs the SCRA. If the results in the determination are inconclusive, the CISO provides the SCRA to the SAOSCRM to make an acceptance or rejection determination. The SAOSCRM provides the signed SCRA to the CISO. Once the CISO has an acceptable determination, the CISO provides the determination to the Cybersecurity SC Assessor. The Cybersecurity SC Assessor provides the final risk determination to the requester and to the Supply Chain Product Risk Technical Review Lead. The flow for a vendor supply chain risk determination is provided in Figure 1.

If the supply chain risk associated with a product in use is found to be unacceptable by the CISO, the CISO notifies the SAOSCRM as soon as possible.

9 SUPPLY CHAIN RISK RESPONSE

If the supply chain risk associated with an ICT product or service NOT already in use is unacceptable, the NRC must NOT acquire the product or service and the NRC Technical Reference Model (TRM) must be updated by the SCPRTRL to indicate acquisition is not permitted.

If the supply chain risk associated with an ICT product or service already in use is unacceptable, the NRC must stop using the ICT product or service as soon as possible, and the NRC TRM must be updated by the SCPRTRL to reflect the determination. The ISSM, in coordination with the project manager, must create a product removal plan and must obtain approval from the CO (if applicable) and CISO on the product removal plan. Once the plan is approved, the ISSM must ensure that product removal occurs in accordance with the plan.

10 SUPPLY CHAIN RISK MONITORING

Supply chain risk monitoring occurs in Tier 3 of CSO-PROS-1323, “Information Security Continuous Monitoring Process” and within CSO-PROS-2102, “System Cybersecurity Assessment Process.”

The ISSO ensures SCRAs and risk determinations are made for new products and services associated with an existing system.

The Information System Security Manager (formerly the ISSO) uses the SCRA service to perform required continuous monitoring, and the SCRA must be updated with a new version as part of continuous monitoring. Unless otherwise specified in the SCRA, a new SCRA must be generated every 7 years.

APPENDIX A ACRONYMS

CISO	Chief Information Security Officer
CNSSI	Committee on National Security Systems Instruction
CO	Contracting Officer
COR	Contracting Officer's Representative
CSO	Computer Security Organization
DCISO	Deputy Chief Information Security Officer
FY	Fiscal Year
GSA	General Services Administration
ICT	Information and Communications Technology
ISSM	Information System Security Manager
ISSO	Information System Security Officer
MD	Management Directive
NDAA	National Defense Authorization Act
NEAT	NRC's Enterprise Acquisition Toolset
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
PL	Public Law
PM	Project Manager
SAOSCRM	Senior Agency Official for Supply Chain Risk Management
SCRA	Supply Chain Risk Assessment
SCRM	Supply Chain Risk Management
SP	Special Publication
TRM	Technical Reference Model

APPENDIX B CRITERIA FOR PRIORITIZING SUPPLY CHAIN RISK ASSESSMENTS FOR ICT PRODUCTS AND SERVICES

Existing ICT products and services for which an SCRA was not performed or for which a new assessment is needed are prioritized for SCRAs in accordance with the table below. If the characteristic applies to an ICT product or service, the associated points are assigned to the ICT product or service. All of the points assigned to the ICT product or service are added up to provide a total prioritization point value. The ICT products or services with the highest point value are assessed first.

ICT Product or Service Characteristic	Points
General use (e.g., dell laptop, Microsoft OS)	20
Includes classified information	10
Includes Safeguards information but not classified information	9
Includes sensitive information, but not classified information or Safeguards information	5
IT infrastructure-wide (e.g., GLINDA)	10
No-cost	3
Used for environmental safety functions	5
Used for financial management functions	8
Used for licensee performance oversight functions	5
Used for Licensing efficiency and effectiveness functions	5
Used for material security functions	8
Used for Mission Essential Function	10
Used for nonproliferation functions	8
Used for proactive risk assessment functions	5
Used for regulatory framework functions	5
Used for special nuclear material control and accounting functions	8

APPENDIX C EXIGER SPECIFIC INFORMATION

Table 2 provides a description of the different types of Exiger reports.

Table 2: Exiger Report Types

Report Type	Report Description
Full Profile	Automated due diligence assessments of entities (persons or companies) utilizing thousands of unstructured sources (open web and news databases) and structured sources (including global watch lists, international government sources, and sanctions lists). DDIQ profiles include premium sources such as BvD , D&B, SecurityScorecard , Google Maps, TLO, ZoomInfo, LexisNexis Corporate, and OpenCorporates. Includes Continuous Monitoring for new regulatory violations, legal proceedings, or other adverse content (Risk scores and assessments available in dashboards)
Enhanced Due Diligence (EDD) Report	Specialized, comprehensive risk and diligence report on a Full Profiled entity, prepared by Exiger's analyst team and incorporating additional sources and research methodologies.
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.

APPENDIX D GLOSSARY

CO_SCR_Vendor_Rev	Information compiled by a contracting officer related to a supplier of an ICT product or service.
DoDI	Department of Defense Instruction
Enhanced Due Diligence Report	Specialized, comprehensive risk and diligence report on a Full Profiled entity, prepared by Exiger's analyst team and incorporating additional sources and research methodologies.
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.
Full Profile	Full Profile: Automated due diligence assessments of entities (persons or companies) utilizing thousands of unstructured sources (open web and news databases) and structured sources (including global watch lists, international government sources, and sanctions lists). DDIQ profiles include premium sources such as BvD , D&B, SecurityScorecard , Google Maps, TLO, ZoomInfo, LexisNexis Corporate, and OpenCorporates. Includes Continuous Monitoring for new regulatory violations, legal proceedings, or other adverse content (Risk scores and assessments available in dashboards)
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.
Information and Communications Technology	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
NDAA Section 889 certification	The fiscal year (FY) 2019 National Defense Authorization Act prohibits agencies from purchasing telecommunications equipment and services produced or provided by specific entities, including all subsidiaries or affiliates and prohibits the government from doing business with entities that use end products produced by these

	companies. This certification indicates that the product and vendor is not prohibited from purchase.
SCR_Offeror_Info	Supply chain risk information provided by a supplier.
SCRA	An NRC created supply chain risk assessment document that identifies an NRC SCR acceptance determination and the rationale supporting the determination.

APPENDIX E REFERENCES

LAWS AND EXECUTIVE ORDERS

[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
[CLINGER]	Clinger-Cohen Act (P.L. 104-106), February 1996, https://www.govinfo.gov/app/details/PLAW-104publ106
[NDAA-889]	FY 2019 National Defense Authorization Act Section 889

POLICIES, REGULATIONS, DIRECTIVES, AND INSTRUCTIONS

[CISA_Defend_SC]	Defending Against Software Supply Chain Attacks
[CISA_SCRM_Essentials]	Supply Chain Risk Management (SCRM) Essentials
[GSA-889-Contractors]	GSA Section 889 Slide Deck that Explains Section 889 to Contractors
[GSA-889-Flyer]	GSA Section 889 Summary Flyer
[GSA-889-Webinar-202009]	Slides from September 10 2020 Section 889 Webinar with GSA Business Line Leaders
[OMB-M-22-18]	M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices
[OMB-M-21-30]	M-22-30, Protecting Critical Software Through Enhanced Security Measures
[ODNI-889-Waiver-Pros]	ODNI Section 889 Waiver Process Flow
[ODNI-SC-Guid-AppC]	ODNI Strategic Supply Chain Security Guidance - Appendix C

STANDARDS, GUIDELINES, AND REPORTS

[FIPS 199]	NIST Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004. https://doi.org/10.6028/NIST.FIPS.199
[FIPS 200]	NIST Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006. https://doi.org/10.6028/NIST.FIPS.200
[SP 800-37]	NIST SP 800-37, Risk Management Framework for Information Systems and Organizations, Revision 2, December 2018. https://doi.org/10.6028/NIST.SP.800-37
[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, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, April 2015. https://doi.org/10.6028/NIST.SP.800-161

NRC DOCUMENTS

[889-Email-Purchase-Card]	Section 889 Certification Email Template for Purchase Card Holders
[889-FAQ-CO-CS]	Section 889 Frequently Asked Questions for Contracting Officers and Contract Specialists
[889-FAQ-Purchase-Card]	Section 889 Frequently Asked Questions (FAQs) for Purchase Card Holders
[889-FAQ-Purchase-Card-IT]	Section 889 Frequently Asked Questions for OCIO Purchase Card Holders & IT Staff
[889-Prov-Clause]	Section 889 Provisions and Clauses Tables
[889-Rep-Form]	Section 889 Representation Form for Purchase Card Holders
[889-SAM-Search]	How to Search SAM to Determine Compliance with Section 889
[889-Template]	Section 889 Compliance Template
[889-Training]	FAC Section 889 Training Slides
[AMD-Info-202008]	AMD Information Digest August 2020 Edition
[CO_SCR_Vendor_Rev]	Supply Chain Risk Assessment (SCRA) Template for Contracting Officers
[CSO-PROS-0007]	CSO-PROS-0007, “Process to Use SCR Investigation Service to Determine ICT Supply Chain Risk Associated with an Offeror”
[CSO-PROS-0009]	CSO-PROS-0009, “Supply Chain Software Evaluation Process”
[CSO-PROS-0011]	CSO-PROS-0011, “Supply Chain Evaluation Process for NDAA Section 889 when Certification not Available”
[CSO-TEMP-0008]	CSO-TEMP-0008, “ICT Supply Chain Risk Assessment Template”
[MD 11.1]	Management Directive 11.1, NRC Acquisition of Supplies and Services
[MD 12.5]	Management Directive 12.5, NRC Cybersecurity Program
[Risk strategy]	NRC Risk Management Strategy, Revision 1.0, ML20266G443
[SCR_Offeror_Info]	Supply Chain Risk Assessment (SCRA) Template for Offerors
[SCRM Strategy]	NRC Supply Chain Risk Management Strategy, Revision 1.0, September 2020, ML20310A085
CSO-PROS-0012	CSO-PROS-0012, “Intake Supply Chain Review and Assessment Process”

CSO-PROS-0008 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
26-Jul-23	1.0	Initial release	Monthly SCRM WG Meetings	None needed.