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

Office Instruction:	**CSO-PROS-0005**
Office Instruction Title:	**Information and Communications Technology Acquisition Process**
Revision Number:	**1.0**
Effective Date:	**February 3, 2021**
Primary Contacts:	**Kathy Lyons-Burke**
Responsible Organization:	**OCIO/CSO**
Summary of Changes:	CSO-PROS-0005, “Information and Communications Technology Acquisition Process,” defines the process that must be used to acquire Information and Communications Technology.
ADAMS Accession No.:	ML20339A376

Agency Official	**Approval Signature and Date**
Jonathan Feibus Chief Information Security Officer (CISO) Office of the Chief Information Officer (OCIO)	Jonathan R. Feibus Digitally signed by Jonathan R. Feibus Date: 2021.02.03 14:20:29 -05'00'

Table of Contents

1 Purpose 1
2 General Requirements 1
3 Information and Communications Technology Acquisition Roles and Responsibilities 2
4 Planning Phase 5
4.1 Define the Requirements 5
4.1.1 Component Requirements 7
4.1.2 System or Service Requirements 8
4.2 Market Research 8
4.3 Determine Acquisition Strategy 8
4.4 Develop Acquisition Plan 8
4.5 Develop Solicitation and Source Selection Process 8
Appendix A Acronyms 10
Appendix B References 12

Computer Security Process
CSO-PROS-0005
Information and Technology Acquisition Process

1 PURPOSE

CSO-PROS-0005 defines the process that must be followed to acquire Information and Communications Technology (ICT) equipment, software, systems, or services. An ITC acquisition is defined in this process as any acquisition where ITC is an element. Several examples of acquisitions that include an ITC element are provided below:

- A service where information is electronically processed by the contractor, such as a contractor that receives electronically recorded voices and transcribes the voice communication into an electronic document.
- A device or piece of hardware where the device performs differently based upon the information provided to it, such as a building Heating, Ventilation, and Air Conditioning (HVAC) or elevator system.
- Electronic storage
- An ITC system or subsystem
- Electronic hardware
- Software

2 GENERAL REQUIREMENTS

This process is required for the following:

- **New Acquisition**: When a new acquisition is undertaken, an assessment of the supply chain risk associated with proposed awardees must be performed.
- **Scope Change Modification**: When there is a modification of an existing contract to change the scope, an assessment of the supply chain risk associated with contractor must be performed.
- **Acquisition Extension**: When an existing contract period of performance is extended, an assessment of the supply chain risk associated with contractor must be performed.
- **Acquisition Option Year**: When an option year of an existing contract is exercised, an assessment of the supply chain risk associated with contractor must be performed.

All NRC ITC acquisitions must be performed in accordance with Management Directive (MD) 11.1, NRC Acquisition of Supplies and Services [MD 11.1] and MD 12.5, NRC Cybersecurity Program.

3 INFORMATION AND COMMUNICATIONS TECHNOLOGY ACQUISITION ROLES AND RESPONSIBILITIES

Table 1 provides the roles and responsibilities associated with NRC ITC acquisition.

Table 1: ITC Acquisition Roles and Responsibilities

Role	Responsibilities
Chief Acquisition Officer (CAO)	• Advises and assists the head of agency and other agency officials to ensure that the mission of the agency is achieved through the management of the agency's acquisition activities • Monitors the performance of acquisition activities and programs • Establishes clear lines of authority, accountability, and responsibility for acquisition decision making within the agency • Manages the direction and implementation of acquisition policy for the agency • Establishes policies, procedures, and practices that promote full and open competition from responsible sources to fulfill best value requirements considering the nature of the property or service procured • Coordinates with other agency officials to ensure that security and privacy requirements are defined in organizational procurements and acquisitions • Works collaboratively with the CIO to implement needed modifications to the ICT acquisition methodology to address Supply Chain Risk Management (SCRM)
Chief Information Officer (CIO)	• Reviews and approves ITC acquisitions • Works collaboratively with the Chief Acquisition Officer (CAO) to identify needed modifications to the ICT acquisition methodology to address risk
Chief Information Security Officer (CISO)	• Ensures cybersecurity requirements are included in ITC acquisitions • Ensures OCIO processes and procedures exist to detect counterfeit and compromised ICT products prior to their deployment • Ensures that the agency enterprise architecture includes ICT risk requirements to facilitate the allocation of ICT controls to agency information systems and the environments in which those systems operate • Ensures that processes used to assess risk incorporate a supply chain risk assessment (SCRA)
Chief Risk Officer (CRO)	• Leads and manages the risk executive (function) in an organization and is responsible for aligning information security and privacy risk management processes with strategic, operational, and budgetary planning processes
Contracting Officer (CO)	• Has delegated authority to enter into, administer, and terminate Government contracts. • Manages contracts and oversees their implementation.

Table 1: ITC Acquisition Roles and Responsibilities

Role	Responsibilities
	• In collaboration with the CISO and CORs, ensures agency's contracting policies and contracts adequately address ICT security requirements.
Contracting Officer's Representative (COR)	• Delegated by the CO to peform certain roles during the administration of the contract (see COR Delegation and Appointment Memordanum for specifics). • Performs contract management activities and functions to ensure contractors meet the commitment of their contracts and proper development of requirements • Has authority to provide technical direction to the contractor as long as that direction is within the scope of the contract • Assists Contracting Officers in managing their contracts • Obtains supply chain certification from the vendor for purchases that are not purchased using Government wide contracts (i.e., GSA) • Monitors the contractor's performance in fulfilling the technical requirements specified.
Enterprise Architect	• Assists with integration of the organizational risk management strategy and system-level security and privacy requirements into program, planning, and budgeting activities, the System Development Life Cycle (SDLC), acquisition processes, security and privacy (including supply chain) risk management, and systems engineering processes
Information Owner	• Establishes the rules for appropriate use and protection of the information and retains that responsibility even when the information is shared with or provided to other organizations
Information System Security Manager (ISSM) – formerly the ISSO	• Serves as a principal advisor on all matters, technical and otherwise, involving the controls for the system • Assists in the development of the system-level security and privacy requirements • 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.
Mission or Business Owner	• Establishes security and privacy requirements that ensure the successful conduct of the organization's missions and business operations
Project Manager (PM)	• Performs program and project management activities and functions in developing accurate government requirements, defining measurable performance standards, and managing life cycle activities to ensure that intended outcomes are achieved • Works with the COR to ensure implementation independent requirements are documented for the acquisition

Table 1: ITC Acquisition Roles and Responsibilities

Role	Responsibilities
Purchase card holders	• Obtain supply chain certification from the vendor for purchases that are outside Government wide contracts (i.e., GSA)
SCRM Working Group	• Identifies security requirements relevant to SCRM. • Identifies contract language that must be included in all acquisitions that have an ICT component that is required to perform the contracted activities. • Ensures that Trade Agreements Act (TAA) compliance is incorporated into all acquisitions.
Security or Privacy Architect	• Ensures that stakeholder protection needs and the corresponding system requirements necessary to protect organizational missions and business functions and individuals' privacy are adequately addressed in the enterprise architecture including reference models, segment architectures, and solution architectures (systems supporting mission and business processes) • Serves as the primary liaison between the enterprise architect and the systems security or privacy engineer and coordinates with system owners, common control providers, and system security or privacy officers on the allocation of controls • Advises authorizing officials, chief information officers, senior accountable officials for risk management or risk executive (function), senior agency information security officers, and senior agency officials for privacy on a range of security and privacy issues
Senior Agency Official for Privacy	• Reviews and approves the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII • Reviews authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information to ensure compliance with privacy requirements and manage privacy risks
Senior Agency Official for Supply Chain Risk Management (SAOSCRM)	• Leads the ICT SCRM Executive Steering Committee (SC). • Leads, with the CAO, a supplier management program.
Supplier Management Program Leads	• Establishes 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, and 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. • Establishes 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.

Table 1: ITC Acquisition Roles and Responsibilities

Role	Responsibilities
	The process includes the ability to leverage other federally accepted supply chain risk reviews.
System Owner	• Works with the COR to ensure documentation of requirements for acquisitions

4 PLANNING PHASE

A COR initiates the ITC acquisition planning phase when a need is identified. There are two (2) high-level categories of ITC acquisition. The first is for a component (e.g., software, hardware, device), and the second is related to system or service implementation. All components must belong to an ITC system or service. Any acquisition will require that funding be allocated to perform the acquisition.

As part of an effort to optimize cost savings and increase ITC transparency, OCIO has developed a new framework to improve the agency's ITC governance processes as required by the Federal Information Technology Acquisition Reform Act (FITARA) and the Clinger-Cohen Act [CLINGER].

The Intake Request is the first step for any ITC-related effort across the NRC and is to help ensure each submitted request for an ITC need is properly reviewed and prioritized. This framework covers two types of requests:

1. NRC Technology Reference Model (TRM) requests are requests to purchase non-standard hardware or software for use at the NRC and is a component request. The list of agency-approved hardware and software, and their related status is available at the TRM link provided above.
2. Architecture changes are projects or activities relating to the development, modernization, or enhancement (DME) of new or existing ITC system(s) or service(s). This request will lead to a new ITC asset or an extensively modified ITC system or service. Examples include:
    a. Projects and activities leading to new ITC assets, systems, or services.
    b. Changes or modifications to existing ITC asset(s) or services that will substantively improve the capability, functionality or performance
    c. Adding or removing other system/service dependencies

4.1 Define the Requirements

Requirements must be documented for an ITC acquisition. The COR must ensure requirements are written in an implementation independent manner using statements that can be used to measure if the component meets the requirement. Implementation dependent statements may be used when there are requirements for compatibility with other implemented solutions.

Part of the requirements definition includes identification of the types of information that will be processed, stored, or transmitted by the item acquired and determining the sensitivity of that information using CSO-PROS-2001, “System Security Categorization Process.” This

determination dictates the cybersecurity requirements that must be met by the acquisition, including requirements for personnel involved in the acquisition. The COR also performs a privacy threshold analysis to determine any privacy implications and if a Privacy Impact Assessment or System of Records Notice is needed.

The CO must include the appropriate local clauses for all acquisitions that cover the following(CO will also complete the CO Acquisitions SCRA check list [SCRA] and the contractor completes SCRA):

1. Offerors shall include the following in their proposal:
    a. Identities of organizations, entities, or tools used for the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of systems and system components.
    b. Development processes used for hardware, software, and firmware
    c. Shipping and handling procedures used for hardware, software, and firmware
    d. Configuration management tools, techniques, and measures to maintain provenance
    e. Personnel and physical security programs associated with individuals with specific roles and responsibilities related to the secure the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of a system or system component
    f. Any other programs, processes, or procedures associated with the production and distribution of supply chain elements

2. All controls/requirements for prime contractors shall also be included in contracts of subcontractors.
3. Providers of systems, system components, or system services shall provide a description of the functional properties of security and privacy controls functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.
4. Providers of systems, system components, or system services shall provide design and implementation information for the controls that includes security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics. The high-level design for the system is expressed in terms of subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules and the interfaces between modules providing security-relevant functionality. Design and implementation documentation shall include manufacturer, version, serial number, verification hash signature, software libraries used, date of purchase or download, and the vendor or download source. Source code and hardware schematics are referred to as the implementation representation of the system.
5. Providers of systems, system components, or system services shall demonstrate the use of a system development life cycle process that includes state-of-the-practice software development methods, systems engineering methods, systems security and privacy engineering methods, and quality control processes
6. Providers of systems, system components, or system services shall

a. Deliver the system, component, or service with NRC-approved security configurations implemented; and
b. Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

7. Providers of systems, system components, or system services shall
    a. Employ only government off-the-shelf or commercial off-the-shelf information assurance and information assurance-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and
    b. Ensure that these products have been evaluated and/or validated by NSA or in accordance with NSA-approved procedures.
8. Providers of systems, system components, or system services shall produce a plan for continuous monitoring of control effectiveness that is consistent with CSO-PROS-1323, Information Security Continuous Monitoring Process [CSO-PROS-1323].
9. Providers of systems, system components, or system services shall identify the functions, ports, protocols, and services intended for organizational use within the proposal or in the design phase at the latest.
10. Providers of systems, system components, or system services shall employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within NRC systems.
11. All information provided by NRC to the contractor is owned by the NRC and may not be used in any way without the expressed consent of the NRC. Providers of systems, system components, or system services shall:
    a. Ensure this information is removed from system components prior to component disposal.
    b. Ensure this information is removed from all contractor systems within 30 days of the end of the contract.
12. Providers of systems, system components, or system services shall establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises; and results of assessments or audits. The providers shall provide NRC the notifications and results within 1 day of receipt of the information.
13. Providers of systems, system components, or system services shall implement a tamper protection program, including counterfeit detection, for the system, system component, or system service throughout the SDLC.

4.1.1 Component Requirements

Once the component need is identified, the COR, in coordination with the office or region, must identify the requirements for the component. Those requirements and the need should be assessed against components NRC already uses to ensure NRC does not already have the capability to meet the need without an acquisition or by obtaining more of a component already in use at NRC. The list of agency-approved hardware and software, and their related status, is available on the TRM.

If the need is not satisfied by components already in use and available at the NRC, the user must submit an IT Business Need request, including the identified requirements. This is the mechanism used for purchase card acquisitions.

4.1.2 System or Service Requirements

Once the system or service need is identified, the office or region must identify the requirements for the need. The office or region then submits a business need request for hardware/software/applications/office 365 that includes the requirements via the OCIO intake process.

4.2 Market Research

In accordance with Federal Acquisition Regulation (FAR) Part 10, the COR identifies in the market research report if requirement has a need for information and communications technology and describes which aspects are subject to SCRM.

4.3 Determine Acquisition Strategy

The CO and COR choose an acquisition strategy in accordance with MD 11.1. For acquisitions over 1 million dollars in total value the Acquisition Strategy is documented in the Strategic Sourcing Group (SSG) paper

4.4 Develop Acquisition Plan

In accordance with FAR Part 7 and MD 11.1, the COR works with the CO to develop an acquisition plan. Once sufficient resources have been identified for the requirement (whether currently available or not), the COR will initiate the acquisition by submitting a requisition in STAQS, either with funding or subject to the availability of funds.

4.5 Develop Solicitation and Source Selection Process

The CO develops a Solicitation and Source Selection Process in accordance with the Federal Acquisition Regulation (FAR) and MD 11.1.

The CO ensures that the SCRA vendor questionnaire is included in the Solicitation as a required submittal.

The CO ensures:

- Prior to Award
  - The source selection criteria includes:
    - Alignment with the NRC cybersecurity framework
    - Responses to the SCRA vendor questionnaire and associated supply chain risk
    - For cloud-based acquisitions:
      - Federal Risk and Authorization Management Program (FedRAMP) authorization

        - In accordance with FAR 239.7602-2, all data must be stored within the United States
    - A product Service Code (PSC) for the solicitation/contract (the COR and CO should consult ODNI's list of PSCs that may post a higher threat to national security) that is appropriate for the requirement
    - Review of the System for Award Management (SAM) for updated registration, certification and representations
    - Documentation of SCRM compliance is included in the summary of negotiations in accordance with FAR Part 12 & 15
- At Contract Award
    - FAR and local clauses that are applicable for cyber security are included

During life cycle of the contract, the COR will ensure that the contractor is in compliance with cyber security requirements and ensures performance of all necessary actions for contracting effectively, complying with the terms and conditions of the contract, and safeguarding the interests of the Government in its contractual relationships and interactions. The COR will notify the CO if any cyber security incident occurs with contractor.

APPENDIX A ACRONYMS

ADM	Office of Administration
CAO	Chief Acquisition Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CO	Contracting Officer
COR	Contracting Officer's Representative
CRO	Chief Risk Officer
CRO	Chief Risk Officer
CSO	Computer Security Organization
DME	Development, Modernization, or Enhancement
ETF	Executive Task Force
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FITARA	Federal Information Technology Acquisition Reform Act
FOCI	Foreign Ownership, Control or Influence
GSA	General Services Administration
HVAC	Heating, Ventilation, and Air Conditioning
ICT	Information and Communications Technology
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ICT	Information and Communications Technology
MD	Management Directive
NIST	National Institute of Standards and Technology

NRC	Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
OEM	Original Equipment Manufacturers
PIV	Personal Identity Verification
PL	Public Law
PM	Project Manager
RFP	Request for Proposal
SAOSCRM	Senior Agency Official for Supply Chain Risk Management
SC	Steering Committee
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SEI	Securing Energy Infrastructure
SP	Special Publication
TAA	Trade Agreement Act
TRM	Technical Reference Model

APPENDIX B 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

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/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf

[OMB A-130] Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[OMB-M-15-14] Office of Management and Budget Memorandum 15-14, Management and Oversight of Federal Information Technology, June 2015 https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2015/m-15-14.pdf

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

Software Assurance in Acquisition: Mitigating Risks to the Enterprise, Software Assurance (SwA) Acquisition Working Group, Mary Linda Polydys and Stan Wisseman, National Defense University, Information Resources Management College, February 2009

Center for Development of Security Excellence (CDSE) Deliver Uncompromised: Supply Chain Risk Management

NRC DOCUMENTS

[CSO-PLAN-0100]	CSO-PLAN-0100, "Enterprise Risk Management Program Plan"
[CSO-PROS-1323]	CSO-PROS-1323, Information Security Continuous Monitoring Process
[CSO-PROS-2001]	CSO-PROS-2001, System Security Categorization Process
[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
[SCRA]	Supply Chain Risk Assessment (SCRA) Template for Contracting Officers
[SCRM Strategy]	NRC Supply Chain Risk Management Strategy, Revision 1.0, September 2020, ML20310A085

CSO-PROS-0005 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
03-Feb-21	1.0	Initial release	Monthly Office Meetings.	None needed.