



**IT Security Procedural Guide:  
Supply Chain Risk Management  
(SR) Controls  
CIO-IT Security-22-120**

**Revision 1**

April 2, 2025

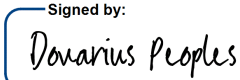
**VERSION HISTORY/CHANGE RECORD**

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		<b>Initial Release –April 14, 2022</b>		
1	Salamon/ Carbonaro	Initial Release.	New guide to provide guidance for NIST SP 800-53, Revision 5, SR controls.	N/A
		<b>Revision 1 - April 2, 2025</b>		
1	Salamon/ Carbonaro/ Normand/ Peralta/ Klemens	Revisions included: <ul style="list-style-type: none"><li>• Updated control parameters to align with the Control Tailoring Workbook (CTW) and Common Control Catalog (CCC).</li><li>• Added leading zeros to controls.</li><li>• Moved CSF categories, Policy, References, and Roles and Responsibilities to Appendices.</li></ul>	Align to the latest GSA guidance.	Throughout

## Approval

IT Security Procedural Guide: Supply Chain Risk Management (SR) controls, CIO-IT Security 22-120, Revision 1, is hereby approved for distribution.

Signed by:



Dovarius Peoples

Acting GSA Chief Information Security Officer

**Contact: GSA Office of the Chief Information Security Officer (OCISO), ICAM Shared Services Division (ISI), C-SCRM Program at [c-scrm@gsa.gov](mailto:c-scrm@gsa.gov).**

Table of Contents

1 Introduction .....1

1.1 Purpose.....2

1.2 Scope.....2

1.3 Policy .....2

1.4 References.....2

2 Roles and Responsibilities.....2

3 GSA Implementation Guidance for SR Controls .....2

3.1 SR-01 Policy and Procedures.....3

3.2 SR-02 Supply Chain Risk Management Plan.....4

3.3 SR-02(01) Supply Chain Risk Management Plan| Establish SCRM Team.....6

3.4 SR-03 Supply Chain Controls and Processes.....7

3.5 SR-05 Acquisition Strategies, Tools, and Methods .....8

3.6 SR-06 Supplier Assessments and Reviews .....8

3.7 SR-08 Notification Agreements .....9

3.8 SR-09 Tamper Resistance and Detection.....10

3.9 SR-09(01) Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle .....10

3.10 SR-10 Inspection of Systems or Components .....11

3.11 SR-11 Component Authenticity.....11

3.12 SR-11(01) Component Authenticity | Anti-Counterfeit Training .....12

3.13 SR-11(02) Component Authenticity | Configuration Control for Component Service and Repair .....13

3.14 SR-12 Component Disposal .....13

4 Summary.....14

Appendix A: CSF Categories/Subcategories .....15

Appendix B: Policy .....17

Appendix C: References.....19

Appendix D: Roles and Responsibilities.....20

Appendix E: Definitions.....23

Table 3-1. Designation of SR Controls .....3

Table 3-2. Designation of SR Control Applicability .....3

Table 3-3. Example Mini Table .....3

Table A-1. CSF Categories/Subcategories and the SR Control Family .....15

Table E-1. Definitions.....23

**Note:** Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a web page or document listed in [Appendix C](#).

## 1 Introduction

General Services Administration (GSA) systems can be subject to cyber supply chain risk through their system lifecycle. Cyber Supply Chain Risk Management (C-SCRM) is a systematic process for managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing response strategies to the risks presented by the supplier, the supplied product, service, and solutions, or the supply chain. The principles and practices described in this guide are focused on the controls from National Institute of Standards and Technology (NIST) including NIST Special Publication (SP) 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations." This guide provides an overview of GSA roles and responsibilities for implementing supply chain risk management (SR) control requirements, SR control applicability per Federal Information Processing Standard (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems" security categorization level, and guidance regarding implementing the SR controls and their requirements. Throughout the remainder of this guide the identifier SR will be used when referring to the supply chain risk management NIST controls or the control family, otherwise SCRM will be used. For the purposes of this guide C-SCRM and SCRM can be considered the same, both terms are used in this guide based on the context where they appear.

This guide relies on C-SCRM guidance from NIST SP 800-53, and preliminary guidance from NIST SP 800-161 Revision 1, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations." As is defined in the aforementioned document, organizations are concerned about the risks associated with products and services that may contain potentially malicious functionality, are counterfeit, tampering, or are vulnerable to compromise due to poor manufacturing and development practices within the cyber supply chain. These risks are associated with an enterprise's decreased visibility into, and understanding of, how the technology that they acquire is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the security, resilience, reliability, safety, integrity, and quality of the products and services.

Every GSA system must follow the practices identified in this guide. Any deviations from the security requirements established in GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy" must be coordinated by the Information System Security Officer (ISSO) through the appropriate Information System Security Manager (ISSM) and authorized by the Authorizing Official (AO). Any deviations, exceptions, or other conditions not following GSA policies and standards must be submitted using the [Security Deviation Request Google Form](#).

Executive Order (EO) 13800, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," requires all agencies to use "[t]he Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by NIST or any successor document to manage the agency's cybersecurity risk." This NIST document is commonly referred to as the Cybersecurity Framework (CSF). GSA uses the NIST SP 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," commonly referred to as the Risk Management Framework (RMF) as its foundation for managing risk, including the implementation of NIST SP 800-53 controls. Further information on how SR controls relate to the CSF is provided in [Appendix A](#).

**Note:** GSA is in the process of developing and updating CIO 2100.1 to align to the CSF 2.0, once that process is completed, the next version of this guide will align to it.

## 1.1 Purpose

The purpose of this guide is to provide guidance for the implementation of SR controls identified in NIST SP 800-53 and SCRM requirements specified in CIO 2100.1. This procedural guide provides GSA Federal employees and contractors with significant security responsibilities (as identified in CIO 2100.1), and other IT personnel involved in the SCRM of IT assets, the specific procedures and processes they are to follow for maintaining GSA systems under their purview.

## 1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who are involved in the C-SCRM of GSA systems and data. All GSA information systems must adhere to the requirements and guidance provided with regard to the procedures, processes, and methods for controlling C-SCRM as described in this guide. Per CIO 2100.1, a GSA system is a system used or operated:

- by the GSA; or
- on behalf of the GSA by a contractor of GSA or by another organization.

Within the scope of this guide, per CIO 2100.1, the following definitions are provided for classifying systems/platforms.

**Contractor System.** An information system in GSA's inventory processing or containing GSA or Federal Information where the infrastructure and/or applications are wholly operated, administered, managed, and maintained by a contractor on behalf of GSA in non-GSA facilities.

**Federal System (i.e., Agency System).** An information system in GSA's inventory processing or containing GSA or Federal information where the infrastructure and/or applications are NOT wholly operated, administered, managed, and maintained by a Contractor.

## 1.3 Policy

[Appendix B](#) contains the CIO 2100.1 policy statements regarding C-SCRM.

## 1.4 References

[Appendix C](#) provides links to references used throughout this guide.

## 2 Roles and Responsibilities

[Appendix D](#) provides a listing of the roles and responsibilities related to implementing, administering, and managing SR controls.

## 3 GSA Implementation Guidance for SR Controls

The GSA-defined parameter settings included in the control requirements are in blue text and offset by brackets in the control text. As stated in [Section 1.2](#), Scope, the requirements outlined within this guide apply to all GSA systems and must be followed by all GSA Federal employees and contractors involved in the C-SCRM of GSA systems and data. The GSA implementation

guidance stated for each control applies to personnel and/or the systems operated on behalf of the GSA. Any additional instructions or requirements for contractor systems will be included in the “Additional Contractor System Considerations” portion of each control section.

Table 3-1 identifies the designation of SR controls as Common, Hybrid, or System-Specific Controls for both Federal and Contractor systems. Effectively, common controls are provided by GSA at the enterprise level or by a GSA Staff Office per its defined SCRM Plan. System specific controls are implemented at each system level, and hybrid controls have shared responsibilities as defined by the SCRM Plan to which each system aligns. CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC), describes the GSA enterprise-wide common and hybrid controls and designates the responsible parties for implementing them.

Table 3-1. Designation of SR Controls

System Type	Federal	Contractor
Common	SR-01, SR-02, SR-02(01), SR-05, SR-06, SR-08, SR-10	
Hybrid	SR-03, SR-11, SR-11(01)	SR-01
System-Specific	SR-09, SR-09(01), SR-11(02), SR-12	SR-02, SR-02(01), SR-03, SR-05, SR-06, SR-08, SR-09, SR-09(01), SR-10, SR-11, SR-11(01), SR-11(02), SR-12

Table 3-2 identifies GSA SR control applicability at the FIPS 199 Low, Moderate, and High levels.

Table 3-2. Designation of SR Control Applicability

FIPS 199 Level	Contractor
Low	SR-01, SR-02, SR-02(01), SR-03, SR-05, SR-08, SR-10, SR-11, SR-11(01), SR-11(02), SR-12
Moderate	SR-01, SR-02, SR-02(01), SR-03, SR-05, SR-06, SR-08, SR-10, SR-11, SR-11(01), SR-11(02), SR-12
High	SR-01, SR-02, SR-02(01), SR-03, SR-05, SR-06, SR-08, SR-09, SR-09(01), SR-10, SR-11, SR-11(01), SR-11(02), SR-12
MiSaaS	SR-06, SR-08

For readers’ ease of use, “mini tables” (see Table 3-3) that contain control/enhancement designation and applicability information are provided at the end of control statements for each SR control. The tables allow readers to see if a control/enhancement is applicable at their system’s FIPS Level/A&A process and if it is common (C), Hybrid (H), or system specific (S), eliminating the need to refer back to Tables 3-1 and 3-2 for this information.

Table 3-3. Example Mini Table

	Low	Mod	High	MiSaaS	Federal	Contractor
Control ID	✓	✓	✓		C	H

3.1 SR-01 Policy and Procedures

- a. Develop, document, and disseminate to [\[personnel with IT security responsibilities as defined in GSA CIO Order 2100.1\]](#):
1. [\[Organization-level\]](#) supply chain risk management policy that:

- (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
- 2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;
- b. Designate an [CISO] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and
- c. Review and update the current supply chain risk management:
  - 1. Policy [annually, as part of CIO 2100.1 update] and following [changes to Federal or GSA policies, requirements, or guidance]; and
  - 2. Procedures [at least every three (3) years] and following [changes to Federal or GSA policies, requirements, or guidance].

	Low	Mod	High	MiSaaS	Federal	Contractor
SR-01	✓	✓	✓		C	H

### Common Control Implementation

The GSA supply chain risk management policy is defined in the GSA Order CIO 2100.1, “GSA Information Technology (IT) Security Policy,” which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for system and information integrity activities. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA’s InSite centralized agency Directives Library.

Supply chain risk management procedures are documented in CIO-IT Security-22-120: Supply Chain Risk Management (SR) Controls. The procedures facilitate the implementation of the supply chain risk management policy and associated controls. This guide is disseminated GSA-wide via GSA’s InSite centralized agency IT Security Procedural Guides.

Per CIO 2100.1, The GSA OCISO is responsible for reviewing and updating:

- 1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance.
- 2. CIO-IT Security-22-120 every three years and following changes to Federal or GSA policies, requirements, or guidance.

### Federal System-Specific Expectation

None, common control.

### Vendor/Contractor System-Specific Expectation

Vendors/Contractors may defer to the GSA policy and guide or implement their own supply chain risk management policies and procedures which comply with GSA’s requirements with the approval of the Authorizing Official (AO) and CISO.

## 3.2 SR-02 Supply Chain Risk Management Plan

- a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [all systems, system components, or system services unless explicitly excluded and approved by the GSA CISO and AO];



- b. Review and update the supply chain risk management plan [biennially] or as required, to address threat, organizational or environmental changes; and
- c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

	Low	Mod	High	MiSaaS	Federal	Contractor
SR-02	✓	✓	✓		C/H*	S

\*Common: GSA IT Managed Federal Systems, Hybrid: Non-GSA IT Managed Federal Systems.

GSA Implementation Guidance

Each documented SCRM Plan describes how the organizational structure governs the SCRM requirements applicable to the high-water mark of the managed information system’s FIPS 199 Level that operate within the operational authority. The plan identifies the formation of the C-SCRM Team that supports the systems within the defined operational authority. The plan identifies any excluded systems, system components, or system services unless explicitly excluded.

Common Control Implementation

GSA IT managed information systems supply chain risk management procedures are defined and documented within CIO-IT Security-21-117: OCISO Cyber Supply Chain Risk Management (C-SCRM) Program. The guide serves as the Tier 2 (organizational) plan for GSA IT consistent with NIST SP 800-161, Revision 1, “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.” The guide identifies how the OCISO C-SCRM Program within the ICAM Shared Services Division (ISI) of GSA IT manages supplier-induced information security risks for GSA IT systems through their lifecycle, including pre-award mitigations and post-award monitoring of risks. The C-SCRM Program’s operational activities are supported by SOPs that detail how the program activities are executed.

CIO-IT Security-21-117 is reviewed/updated biennially upon changes to Federal or GSA policies requirements or guidance. ISI ensures the program’s SOPs are updated biennially.

ISI SOPs are stored within Google Shared Drives that have restricted access. Note: CIO-IT Security-21-117 is a public document and does not require protection.

GSA IT Managed Federal System-Specific Expectation

None, Common Control.

Non-GSA IT Managed Federal System-Specific Expectation

Non-GSA IT managed information systems must have their own system-specific Supply Chain Risk Management Plan that details response activities and reporting requirements to GSA consistent with NIST SP 800-161 and CIO-IT Security-21-117. As identified by NIST SP 800-161, organizations can develop Tier 2 plans that are inherited by systems within their control. A System Security and Privacy Plan (SSPP) can serve as a Tier 3 plan for any organization with a Tier 2 plan.

Vendor/Contractor System-Specific Expectation

Vendors/Contractors are required to have their own system-specific or organizational Supply Chain Risk Management Plan that details response activities and reporting requirements to GSA consistent with NIST SP 800-161. Per NIST SP 800-161, organizations can develop Tier 2 plans that are inherited by their managed systems. A System Security and Privacy Plan (SSPP) can serve as a Tier 3 plan for any organization with a Tier 2 plan.

3.3 SR-02(01) Supply Chain Risk Management Plan| Establish SCRM Team

Establish a supply chain risk management team consisting of [Internal GSA: SCRM Senior Accountable Official and SCRM Executive Board and SCRM Working Group members, as defined in the SCRM Executive Board Charter, External: GSA SSO or Contractor recommended personnel, roles, and responsibilities as approved by the GSA CISO and AO] to lead and support the following SCRM activities: [Internal GSA: defined in the SCRM Executive Board Charter, External: organization-defined supply chain risk management activities].

	Low	Mod	High	MiSaaS	Federal	Contractor
SR-02(01)	✓	✓	✓		C/H*	S

\*Common: GSA IT Managed Federal Systems, Hybrid: Non-GSA IT Managed Federal Systems.

GSA Implementation Guidance

System Owners establish a SCRM Team for their system or organization to implement the C-SCRM Plan for their system or organization consistent with NIST SP 800-161. Each documented SCRM Plan describes how the organizational structure governs the SCRM requirements applicable to the high-water mark of the managed information system’s FIPS 199 Level that operate within the operational authority. The plan identifies the formation of the SCRM Team that supports the systems within the defined operational authority.

Common Control Implementation

As defined by [GSA’s SCRM Executive Board Charter](#), GSA has established a supply chain risk management team consisting of SCRM Senior Accountable Officials who form GSA’s SCRM Executive Board. The board provides oversight to any GSA SCRM working group(s) established to accomplish the following SCRM activities:

- Analyze GSA’s supply chain and use risk-based approaches to address supply chain risks (including, but not limited to emerging risk information related to communications technology) to inform strategic and operational management decisions and investments.
- Ensure policy development and resource management efforts include planning for and consideration of incident management, contingency, continuity, and response requirements.
- Facilitate the coordinated alignment of GSA’s Government-wide responsibilities (e.g., policy, training, shared services, interagency engagement, customer agency-facing service, product offerings, real estate) with the internal GSA Enterprise responsibilities to safeguard and manage risk to GSA’s mission and its portfolio of assets.
- Integrate SCRM policies, processes, and oversight activities into GSA’s internal acquisition processes and information and communication technology (ICT) investment and lifecycle management processes.
- Provide guidance to internal GSA employees on supply chain risks and incorporate SCRM-relevant responsibilities and duties, where applicable.
- Develop processes and procedures for supporting implementation of new statutory and regulatory requirements related to SCRM.
- Develop processes and procedures for interfacing with external stakeholders on SCRM issues as defined in the SCRM Executive Board Charter. Stakeholders include the Federal Acquisition Security Council (FASC) Information Sharing, and Risk Management Task Force and the Department of Homeland Security ICT SCRM Working Group.

The OCISO C-SCRM Team that exists within the ICAM Shared Services Division (ISI) serves as the C-SCRM Team for all GSA IT systems.

**GSA IT Managed Federal System-Specific Expectation**

None, Common Control.

**Non-GSA IT Managed Federal System-Specific Expectation**

Establish a SCRM Team for the managed system(s) or organization for implementing a SCRM plan for the managed system(s) or organization consistent with NIST SP 800-161, Revision 1, “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.”

**Vendor/Contractor System-Specific Expectation**

Vendors/contractors must establish their own system-specific SCRM Team to lead and support the system’s SCRM activities consistent with NIST SP 800-161.

**3.4 SR-03 Supply Chain Controls and Processes**

- a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [GSA systems and their components] in coordination with [SSO or contractor recommended supply chain personnel as approved by the GSA CISO and AO];
- b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [SCRM controls (based on FIPS 199 Baseline) identified in the GSA CTW]; and
- c. Document the selected and implemented supply chain processes and controls in [security and privacy plans].

	Low	Mod	High	MiSaaS	Federal	Contractor
SR-03	✓	✓	✓		H	S

**GSA Implementation Guidance**

Each system’s SCRM Plan should cover the full SDLC of systems and programs, including research and development, design, manufacturing, acquisition, delivery, integration, operations, and disposal/retirement.

Systems identify their respective Service and Staff Office’s SCRM Plan or Responsible IT Organization’s SCRM Plan they align to. Each system is required to document how it performs its Hybrid and System-Specific control requirements.

**Common Control Implementation**

The OCISO Cyber Supply Chain Risk Management (C-SCRM) Team maintains a list of critical suppliers for GSA IT systems and acquisitions by reviewing various data sources as identified in the team's SOPs. Identified critical suppliers are subjected to further investigation for cyber supply chain risks through an established monitoring process identified in the C-SCRM team’s SOP. The goal of supplier reviews is to uncover supply chain weaknesses or deficiencies in a risk-based manner and escalate significant risks.

GSA’s system specific NIST SP 800-53, Revision 5, “Security and Privacy Controls for Information Systems and Organizations” security control requirements related to the protection against supply chain operational risks are defined by the OCISO C-SCRM Team. Control selection applicability is based on the system's FIPS-199 security impact levels and GSA’s defined baselines, per CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk. The specific control selections are documented within the GSA Control Tailoring Workbook (CTW),

which defines the agency’s control selection parameters and the baseline’s applicable security controls documentation requirements.

System Owners, ISSOs, and ISSMs are responsible for documenting and maintaining their managed information system’s SSPP per the GSA CTW and based on the system’s baseline documentation requirements.

**Federal System-Specific Expectation**

System Owners, ISSOs, and ISSMs are responsible for ensuring their managed systems’ System Security and Privacy Plans (SSPPs) are aligned with the GSA CTW and their systems’ selected baseline documentation requirements.

**Vendor/Contractor System-Specific Expectation**

Vendors/Contractors must establish their own system-specific Supply Chain control parameters and processes consistent with NIST SP 800-161, Revision 1, “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.” Each Vendor/Contractor owned/operated system is required to align its SSPP security control requirements with NIST 800-53 security control selections as detailed in the GSA CTW.

**3.5 SR-05 Acquisition Strategies, Tools, and Methods**

Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [[Federal: acquisition strategies, contract tools, and procurement methods as defined on the SCRM SAO & Review Board Webpage](#), [Contractor: organization-defined acquisition strategies, contract tools, and procurement methods](#)].

	Low	Mod	High	MiSaaS	Federal	Contractor
SR-05	✓	✓	✓		C	S

**Common Control Implementation**

GSA acquisition requirements are defined in the General Services Administration Acquisition Manual (GSAM), consistent with Federal Acquisition Regulations. These requirements are defined by the SCRM SAO and SCRM Review Board and are detailed on GSA’s internal Cyber Supply Chain Risk Management (C-SCRM) web page.

**Federal System-Specific Expectation**

None, Common Control.

**Vendor/Contractor System-Specific Expectation**

Vendors/Contractors must employ their own system-specific or organization-wide acquisition strategies, tools, and methods consistent with NIST SP 800-161, Revision 1, “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.”

**3.6 SR-06 Supplier Assessments and Reviews**

Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [[annually](#)].

	Low	Mod	High	MiSaaS	Federal	Contractor
SR-06		✓	✓	✓	C/H*	S

\*Common: GSA IT Managed Federal Systems, Hybrid: Non-GSA IT Managed Federal Systems.

**GSA Implementation Guidance**

Annually, the identified supporting C-SCRM team assesses and reviews the supply chain-related risks associated with the suppliers or contractors of the supported systems within the organization’s defined operational authority.

**Common Control Implementation**

The OCISO Cyber Supply Chain Risk Management (C-SCRM) team develops, maintains, and annually updates a list of critical suppliers for GSA IT. The list is based on input from various sources for GSA-IT managed systems and includes software inventories, hardware inventories, and financials related to acquisitions. Supply chain risks that are unique for the most critical vendors are then incorporated into final determinations. For the resultant set of critical vendors, supplier assessments are conducted, and significant risks are addressed. The specific controls for maintaining the critical supplier list and conducting supplier reviews are identified within the C-SCRM Program’s SOPs.

**GSA IT Managed Federal System-Specific Expectation**

None, Common Control.

**Non-GSA IT Managed Federal System-Specific Expectation**

System Owners must establish a process and perform system-specific or organization-wide Supplier Assessments and Reviews consistent with NIST SP 800-161, Revision 1, “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.”

**Vendor/Contractor System-Specific Expectation**

Vendors/Contractors must establish a process and perform system-specific or organization-wide supplier assessments and reviews consistent with NIST SP 800-161.

**3.7 SR-08 Notification Agreements**

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; results of assessments or audits].

	Low	Mod	High	MiSaaS	Federal	Contractor
SR-08	✓	✓	✓	✓	C/H*	S

\*Common: GSA IT Managed Federal Systems, Hybrid: Non-GSA IT Managed Federal Systems.

**GSA IT Managed Federal System Common Control Implementation**

The GSAM establishes requirements for reporting and handling of cyber supply chain events for GSA, including supply chain compromises. For GSA IT managed systems, the OCISO C-SCRM team has established processes for escalating supply chain events and incidents within C-SCRM SOPs, including the distribution of GSA supplier assessment results and C-SCRM events or incidents.

**Non-GSA IT Managed Federal System Common Control Implementation**

The GSAM establishes requirements for reporting and handling of cyber supply chain events and incidents for GSA, including supply chain compromises.

**GSA IT Managed Federal System-Specific Expectation**

None, Common Control.

**Non-GSA IT Managed Federal System-Specific Expectation**

System Owners must establish system-specific notification agreements and procedures consistent with NIST SP 800-161, Revision 1, “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.”

**Vendor/Contractor System-Specific Expectation**

Vendors/Contractors must establish system-specific or organization-wide Notification Agreements and procedures consistent with NIST SP 800-161.

**3.8 SR-09 Tamper Resistance and Detection**

Implement a tamper protection program for the system, system component, or system service.

	Low	Mod	High	MiSaaS	Federal	Contractor
SR-09			✓		S	S

**GSA Implementation Guidance**

Anti-tamper technologies, tools, and techniques provide a level of protection for systems, system components, and services against many threats, including reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components during distribution and when in use. Organizations use a combination of hardware and software techniques for tamper resistance and detection. Organizations use obfuscation and self-checking to make reverse engineering and modifications more difficult, time-consuming, and expensive for adversaries. The customization of systems and system components can make substitutions easier to detect and therefore limit damage.

**Federal System-Specific Expectation**

System Owners must implement a protection program to define which systems, system components, or system services must be tested for tampering and tampering resistance.

**Vendor/Contractor System-Specific Expectation**

Vendor/contractor owned/operated systems must implement a protection program to define which systems, system components, or system services must be tested for tampering and tampering resistance. The implemented protection program must be consistent with NIST SP 800-161.

**3.9 SR-09(01) Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle**

Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.

	Low	Mod	High	MiSaaS	Federal	Contractor
SR-09(01)			✓		S	S

**Federal System-Specific Expectation**



System Owners must employ anti-tamper technologies, tools, and techniques for use by system developers and require they be used throughout the SDLC.

### Vendor/Contractor System-Specific Expectation

Vendor/contractor owned/operated systems must employ anti-tamper technologies, tools, and techniques for use by system developers and require they be used throughout the SDLC. The employed technologies, tools, and techniques must be consistent with NIST SP 800-161.

## 3.10 SR-10 Inspection of Systems or Components

Inspect the following systems or system components [at a frequency as identified by the Supply Chain Risk Management Team as identified in SR-02(01)] to detect tampering: [systems or system components as identified by the Supply Chain Risk Management Team as identified in SR-02(01)].

	Low	Mod	High	MiSaaS	Federal	Contractor
SR-10	✓	✓	✓		C/H*	S

\*Common: GSA IT Managed Federal Systems, Hybrid: Non-GSA IT Managed Federal Systems.

### GSA Implementation Guidance

The inspection of systems or systems components for tamper resistance and detection addresses physical and logical tampering and is applied to systems and system components removed from organization-controlled areas. Indications of a need for inspection include changes in packaging, specifications, factory location, or entity in which the part is purchased, and when individuals return from travel to high-risk locations.

### Common Control Implementation

The OCISO Cyber Supply Chain Risk Management (C-SCRM) team uses a risk-based approach to identify which system components are inspected and at which frequency. When identified, a third-party service evaluates the products for evidence of compromise to determine if counterfeit components or parts from companies subject to prohibitions are included.

### GSA IT Managed Federal System-Specific Expectation

None, Common Control.

### Non-GSA IT Managed Federal System-Specific Expectation

System Owners must establish system-specific processes to inspect components for tampering consistent with NIST SP 800-161, Revision 1, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations."

### Vendor/Contractor System-Specific Expectation

Vendors/contractors must establish system-specific or organization-wide processes to inspect components for tampering consistent with NIST SP 800-161.

## 3.11 SR-11 Component Authenticity

- Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and
- Report counterfeit system components to [the source of the counterfeit component; Federal: GSA SCRM Review Board and as a security incident to the IT Service Desk in accordance with IR-06 and GSAM-2021-511, Contractor: Contracting Officer].

	Low	Mod	High	MiSaaS	Federal	Contractor
SR-11	✓	✓	✓		H	S

### GSA Implementation Guidance

Sources of counterfeit components include manufacturers, developers, vendors, and contractors. Anti-counterfeiting policies and procedures support tamper resistance and provide a level of protection against the introduction of malicious code.

### Common Control Implementation

CIO 2100.1, “GSA Information Technology (IT) Security Policy,” requires anti-counterfeit procedures be developed to include detection of counterfeit hardware or software components consistent with NIST SP 800-53, Revision 5, if applicable.

System Owners, ISSOs and ISSMs or system custodians on behalf of their System Owner are advised, per the GSAM and GSA’s Incident Reporting (IR-06) guidance, to report the detection of a counterfeit system component to the GSA IT Service Desk as an incident.

### Federal System-Specific Expectation

System Owners must establish system-specific Component Authenticity procedures consistent with NIST SP 800-161, Revision 1, “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.”

### Vendor/Contractor System-Specific Expectation

Vendor/Contractor owned/operated systems must establish system-specific or organization-wide Component Authenticity policy and procedures consistent with NIST SP 800-161 and report counterfeit system components to their GSA Contracting Officer.

## 3.12 SR-11(01) Component Authenticity | Anti-Counterfeit Training

Train [\[the SCRM Team as identified in SR-02\(01\) and personnel associated with installing hardware components for GSA systems annually and upon entry\]](#) to detect counterfeit system components (including hardware, software, and firmware).

	Low	Mod	High	MiSaaS	Federal	Contractor
SR-11(01)	✓	✓	✓		H	S

### GSA Implementation Guidance

Organizations are to establish and maintain anti-counterfeiting training material and require personnel within their organization who install hardware components to complete the training annually or upon entry into the organization. Training must include means of reporting detected counterfeit components to meet SR-11 control expectation.

### Common Control Implementation

GSA OCISO has established “Detecting Counterfeit Products” training. This anti-counterfeit training has been made available to all personnel who have a role in security operations, system development, and who perform the installation of IT components on behalf of a System Owner at GSA. The training is available to all personnel with access to GSA Online University and covers detection of counterfeit system components for software, hardware, and firmware.



**Federal System-Specific Expectation**

System Owners must identify staff who perform the installation and development of IT system components (including hardware, software, and firmware) per their managed system boundary. System Owners must ensure their identified staff complete the anti-counterfeit training available on GSA Online University upon onboarding and annually thereafter.

**Vendor/Contractor System-Specific Expectation**

Vendor/contractor owned/operated systems must perform system-specific anti-counterfeit training consistent with NIST SP 800-161, Revision 1, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations."

**3.13 SR-11(02) Component Authenticity | Configuration Control for Component Service and Repair**

Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: [\[all components\]](#).

	Low	Mod	High	MiSaaS	Federal	Contractor
SR-11(02)	✓	✓	✓		S	S

**Federal System-Specific Expectation**

System Owners ensure managed system components are maintained under configuration control. Maintaining configuration control of the system's components ensures the successful return to service upon completion of repair or servicing. Examples could be ensuring that there is data encryption when servicing hardware or wiping devices before they are sent out for repair.

**Vendor/Contractor System-Specific Expectation**

Vendors/contractors are required to comply with the control statements. Vendor/contractor owned/operated systems must establish their own system-specific Supply Chain Controls and Processes consistent with NIST SP 800-161.

**3.14 SR-12 Component Disposal**

Dispose of [\[data, documentation, tools, and system components in accordance with the Media Protection procedural guide or Contractor recommendation as approved by the GSA CIO and AO\]](#) using the following techniques and methods: [\[as described in the Media Protection procedural guide or Contractor recommendation as approved by the GSA CIO and AO\]](#).

	Low	Mod	High	MiSaaS	Federal	Contractor
SR-12	✓	✓	✓		S	S

**Federal System-Specific Expectation**

System Owners must ensure system's data, documentation or system components are disposed of properly and in accordance with CIO-IT Security 06-32: Media Protection (MP). Disposal activities are performed throughout the lifecycle of a managed information system. Opportunities for compromise during disposal affect physical and logical data, including system documentation in paper-based or digital files; shipping and delivery documentation; memory sticks with software code; or complete routers or servers that include permanent media, which contain sensitive or proprietary information.

**Vendor/Contractor System-Specific Expectation**

Vendor/contractor owned/operated systems must establish their own system-specific procedures, techniques and methods for disposing of data, documentation, tools, and system components. Vendors may follow the guidance in CIO-IT Security 06-32 when preparing their procedures, techniques, and methods.

## **4 Summary**

SR controls are required to ensure the confidentiality, integrity, availability, accountability and assurance of IT resources and facilities.

Effective SR controls established and implemented for GSA's IT resources assist the agency in accomplishing the stated mission, complying with federal mandates and the GSA IT Security Policy. Once effective controls have been established, they must be maintained through an ongoing effort and continuously monitored to ensure that the access controls remain effective in mitigating risks. Where there is a conflict between NIST guidance and GSA guidance, contact the OCISO, ISP Division for guidance, at [ispcompliance@gsa.gov](mailto:ispcompliance@gsa.gov).

## Appendix A: CSF Categories/Subcategories

The CSF focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The core of the CSF consists of five concurrent and continuous Functions—Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). The CSF complements, and does not replace, an organization's risk management process and cybersecurity program. GSA uses NIST's Risk Management Framework (RMF) from NIST SP 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy." Table A-1, CSF Categories/Subcategories and the NIST SR Control Family, lists the Categories and Subcategories from the CSF that are supported by the implementation of policies, procedures, and processes from the NIST SP 800-53 Revision 5 SR control family<sup>1</sup>. CIO 2100.1 and this procedural guide provide GSA's policies and procedural guidance regarding C-SCRM for GSA information systems and implementation of the SR controls.

**Table A-1. CSF Categories/Subcategories and the SR Control Family**

CSF Category/Subcategory Identifier	Definition/Description
<b>Business Environment (ID.BE):</b> 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.	<p><b>ID.BE-1:</b> The organization's role in the cyber supply chain is identified and communicated. SR-01, SR-03</p> <p><b>ID.BE-4:</b> Dependencies and critical functions for delivery of critical services are established. SR-02</p>
<b>Governance (ID.GV):</b> The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	<p><b>ID.GV-1:</b> Organizational cybersecurity policy is established and communicated. SR-01</p> <p><b>ID.GV-3:</b> Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. SR-01</p>
<b>Supply Chain Risk Management (ID.SC):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	<p><b>ID.SC-1:</b> Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders. SR-01, SR-02, SR-03, SR-05</p> <p><b>ID.SC-2:</b> Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process. SR-02, SR-03, SR-05, SR-06</p> <p><b>ID.SC-3:</b> Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. SR-02, SR-03, SR-05</p>

<sup>1</sup>Derived from [CSF 1.1 to SP 800-53 r5 Mappings](#).

CSF Category/Subcategory Identifier	Definition/Description
<b>Information Protection Processes and Procedures (PR.IP):</b> 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.	<b>PR.IP-6:</b> Data is destroyed according to policy. SR-12
<b>Detection Processes (DE.DP):</b> Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	<b>DE.DP-2:</b> Detection activities comply with all applicable requirements SR-01, SR-09, SR-10
<b>Analysis (RS.AN):</b> Analysis is conducted to ensure effective response and support recovery activities.	<b>RS.AN-5:</b> Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers). SR-06

## Appendix B: Policy

The following extracts from CIO 2100.1 contain information related to C-SCRM.

### Chapter 3, Policy for Identify Function.

#### 2. Business Environment.

a. GSA's role within the supply chain is: (1) as a consumer of supplies from vendors/providers for its internal systems and use; and (2) as an acquisition agency dedicated to procuring goods and services for the Federal Government, as well as providing acquisition, technical, and project management services to assist agencies in acquiring and deploying information technology and professional services solutions.

b. In both of these roles, requiring activities, working with their COs must ensure supply chain risk management is included in contracts where appropriate, and acquirers must determine whether the acquisition risk is acceptable given their system's environment.

#### 6. Supply Chain Risk Management.

a. The OCISO Cyber Supply Chain Risk Management (C-SCRM) Program addresses cyber risks both prior to and post contract award for information and computer technology (ICT) products and services. Accordingly, all GSA systems must manage risks to their cyber supply chain IAW:

- (1) CIO-IT Security-21-117, OCISO Cyber Supply Chain Risk Management (C-SCRM) Program;
- (2) CIO-IT Security-22-120, Supply Chain Risk Management (SR) Controls;
- (3) CIO-IT Security-09-48, Security Language for IT Acquisition Efforts; and
- (4) NIST SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.

b. Cyber Supply Chain events must be reported to the GSA IT Service Desk IAW GSAM Part 504.7005, Notification procedures for cyber-supply chain events.

c. Acquisition professionals must consider potential cyber supply chain risks as part of the acquisition process as follows:

- (1) IAW GSAM Part 504.7005.
- (2) When applicable, if the original equipment manufacturer (OEM) has a program to authorize both the product's pricing and sale by a third-party vendor, proof of the bidder's authorized standing with the OEM is required prior to any business-award.

d. Systems, their suppliers and third-party suppliers must comply with:

- (1) Public Law 115-91, National Defense Authorization Act for Fiscal Year 2018, Section 1634, Prohibition on Use of Products and Services Developed or Provided by Kaspersky Lab, which prohibits the use of any hardware, software, or services developed or provided in whole or in part by— (1) Kaspersky Lab (or any successor entity), (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab, or (3) any entity of which Kaspersky Lab has majority ownership.
- (2) Federal Acquisition Regulation (FAR) 52.204-25. It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232) the procuring or obtaining or extending or renewing a contract to procure or obtain equipment or services produced or provided by the following organizations

unless an exception or waiver is granted per the law or the FAR; (1) Huawei Technologies Company, (2) ZTE Corporation, (3) Hytera Communications Corporation, (4) Hangzhou Hikvision Digital Technology Company, (5) Dahua Technology Company, and any subsidiary or affiliate of these companies.

(3) FAR 52.204-27 which prohibits under Section 102 of the Consolidated Appropriations Act 2023, Public Law 117-328, the presence or use of TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited from being used on any information technology as defined in 40 U.S.C. § 11101(6).

(4) Actions specified in Federal mandates, including but not limited to Federal Laws, Executive Orders, OMB Memoranda, and Cybersecurity Directives when the mandate is applicable to their system or the components therein. System and organizational personnel shall provide data to support compliance with the applicable Federal mandates as requested.

e. Appropriate personnel (e.g., Requiring Official, CO, COR) must assess a supplier's and third-party partner's supply chain prior to acquisition as part of contract requirements and as necessary thereafter. Assessments may consist of audits, tests, or other forms of evaluation as deemed necessary.

f. All information systems must develop anti-counterfeit procedures that include detection of counterfeit hardware or software components consistent with NIST SP 800-53, Revision 5.

g. Internet of Things (IoT) devices cannot be procured unless a review of the contract by the CIO identifies that it complies with NIST SP 800-213 or the CIO grants a waiver under one of the conditions of the IoT Act. Any waivers must include the elements identified in the IoT Act and be sent to the GSA Administrator.

## Appendix C: References

### Federal Laws, Standards, Regulations, and Publications:

- [EO 13800](#), Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- [FIPS PUB 199](#), Standards for Security Categorization of Federal Information and Information Systems
- [NIST CSF](#), Framework for Improving Critical Infrastructure Cybersecurity
- [NIST SP 800-37, Revision 2](#), Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- [NIST SP 800-53, Revision 5](#), Security and Privacy Controls for Information Systems and Organizations
- [NIST SP 800-161, Revision 1](#), Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
- [Federal Acquisition Regulation \(FAR\) 52.204-25](#), Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment
- [Public Law 115-91](#), National Defense Authorization Act for Fiscal Year 2018

### GSA Policies, Procedures, Guidance:

- [GSA Order CIO 2100.1](#), GSA Information Technology (IT) Security Policy
- [GSA Acquisition Manual \(GSAM\)](#)

The GSA CIO-IT Security Procedural Guides listed below are available on the GSA.gov [IT Security Procedural Guides](#) page with the exception of CIO-IT Security-Privacy-18-90. It is available on the internal GSA InSite [IT Security Procedural Guides](#) page.

- CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk
- CIO-IT Security-06-32: Media Protection (MP)
- CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts
- CIO-IT Security-09-44: Plans of Action & Milestones (POA&M)
- CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC)
- CIO-IT Security-21-117: Cyber Supply Chain Risk Management OCISO (C-SCRM) Program

## Appendix D: Roles and Responsibilities

System Owners have direct responsibility to ensure effective implementation and management of GSA's C-SCRM control requirements for each of their systems. The roles and responsibilities provided in this section have been extracted or paraphrased from CIO 2100.1 or summarized from GSA and Federal guidance. Throughout this guide requirements for implementing C-SCRM controls are described. Complete roles and responsibilities for agency management officials and roles with significant IT Security responsibilities are defined in CIO 2100.1.

### GSA Chief Information Security Officer (CISO)

FISMA establishes the designation of a Senior Agency Information Security Officer. GSA has assigned that responsibility to the CISO. Responsibilities specifically regarding SR controls and C-SCRM include:

- Managing the development, documentation, and dissemination of the C-SCRM policy and procedures;
- Establishing policies to coordinate C-SCRM incident response for GSA IT systems;
- Establishing and serving as GSA-lead for development, implementation, and ongoing operational management of Tier 3 level C-SCRM policies, plan(s), processes, and controls.

### Federal Acquisition Service (FAS) Commissioner

The Federal Acquisition Service (FAS) Commissioner acts as GSA's Senior Accountable Official (SAO) for C-SCRM. The alternate is the Chief Acquisition Officer.

### Supply Chain Risk Management (SCRM) Review Board

GSA's SCRM Review Board is responsible for considering questions related to emerging policy changes and acquisition requirements resulting from Supply Chain Event Reports and Contracting Officer inquiries.

### Authorizing Officials (AOs)

Authorizing Officials are the officials with the authority to formally assume responsibility for operating a system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Responsibilities include:

- Reviewing and approving security safeguards of systems and issuing Authorization to Operate (ATO) approvals for each system under their purview based on the acceptability of the security safeguards of the system (risk-management approach);
- Ensuring that GSA systems under their purview have implemented the required SR controls in accordance with GSA and Federal policies and requirements;
- Ensuring a plan of action and milestones (POA&M) item is established and managed to address SR Controls that are not fully implemented.

### System Owners (SOs)

System Owners are management officials within GSA with responsibility for the acquisition, development, maintenance, implementation, and operation of GSA's IT systems. Primary responsibility for managing risk should rest with the System Owners. Responsibilities include:



- Ensuring systems and the data each system processes have necessary security controls in place and are operating as intended and protected IAW GSA regulations and any additional guidelines established by the OCISO and relayed by the ISSO or ISSM;
- Obtaining the resources necessary to securely implement and manage their respective systems;
- Consulting with the ISSM and ISSO and receiving the approval of the AO, when selecting the mix of controls, technologies, and procedures that best fit the risk profile of the system;
- Coordinating with IT security personnel, including the ISSM and ISSO and Data Owners, to ensure the maintenance the system security plan and implementation of system and data security requirements;
- Working with the ISSO and ISSM to develop, implement, and manage POA&Ms for their respective systems IAW GSA CIO-IT Security-09-44.

### Information System Security Officers (ISSOs)

ISSOs are responsible for ensuring implementation of adequate system security in order to prevent, detect, and recover from security breaches. Responsibilities include:

- Ensuring the system is operated, used, maintained, and disposed of IAW documented security policies and procedures. Necessary security controls should be in place and operating as intended;
- Advising System Owners of risks to their systems and obtaining assistance from the ISSM, if necessary, in assessing risk;
- Assisting System Owners in completing and maintaining the appropriate A&A documentation as specified in GSA CIO-IT Security-06-30;
- Developing POA&Ms regarding SR controls for all systems under their purview.

### Information System Security Managers (ISSMs)

ISSMs serve as intermediary to System Owners and the OCISO Director responsible for ISSO services. Responsibilities include:

- Providing guidance, advice, and assistance to ISSOs on IT security issues, the IT Security Program, and security policies;
- Ensuring A&A support documentation is developed and maintained for the life of the system;
- Forwarding to the applicable OCISO Director, copies of A&A documents to be signed by the appropriate individuals as required in A&A guidance;
- Supporting the security measures and goals established by the CISO.

### Suppliers and Third-Party Partners

Suppliers and third-party partners must abide by all GSA IT Security Procedural Guides which incorporate supply chain guidance as provided in NIST guidance IAW GSA CIO-IT Security-09-48. Responsibilities include:

- Compliance with Section 1634 of Public Law 115-91, which prohibits the use of goods or services associated with Kaspersky Lab;
- Compliance with 52.204-25 of the Federal Acquisition Regulation (FAR), which prohibits specific telecommunications equipment.

## **Contracting Officers and Representatives**

The CO/COR function is responsible for managing contracts and overseeing their implementation. Responsibilities include:

- Collaborating with the CISO or other appropriate official to ensure that the agency's contracting policies adequately address the agency's information security requirements;
- Coordinating with the CISO or other appropriate official as required ensuring that all agency contracts and procurements are compliant with the agency's information security policy, and include appropriate security contracting language and security requirements in each contract;
- Ensuring contracts and task orders for ISSM and ISSO services include performance requirements that can be measured;
- Ensuring new solicitations for all GSA IT systems include the security contract language from GSA CIO-IT Security-09-48.

## Appendix E: Definitions

Table E-1 identifies terms and the definitions used in this guide.

**Table E-1. Definitions**

Term	Definition
Risk ( <a href="#">NIST Glossary</a> )	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the circumstance or event occurs; and the likelihood of occurrence.
Risk Assessment ( <a href="#">NIST Glossary</a> )	The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.
Risk Management ( <a href="#">NIST Glossary</a> )	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
Cyber-Supply Chain Risk Management (C-SCRM) ( <a href="#">GSAM Definitions</a> )	Management of cyber-related (or, more generally, technology-related) risks in all phases of the acquisition lifecycle and at all levels of the supply chain, regardless of the product(s) or service(s) procured.
Supplier ( <a href="#">NIST Glossary</a> )	Organization or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain, developers or manufacturers of systems, system components, or system services; systems integrators; vendors; product resellers; and third party partners.
Cyber-Supply Chain Event ( <a href="#">GSAM Definitions</a> )	Any situation or occurrence in or to a network, information system, or within the supply chain, not purchased on behalf of another agency, that has the potential to cause undesirable consequences or impacts.
Contractor System ( <a href="#">CIO 2100.1</a> )	An information system in GSA's inventory processing or containing GSA or Federal information where the infrastructure and/or applications are wholly operated, administered, managed, and maintained by a contractor on behalf of GSA in non-GSA facilities.
Federal System (i.e., Agency System) ( <a href="#">CIO 2100.1</a> )	An information system in GSA's inventory processing or containing GSA or Federal information where the infrastructure and/or applications are NOT wholly operated, administered, managed, and maintained by a Contractor.