



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

Revision 2

October 1, 2026

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Initial Release –April 14, 2022		
1	Salamon/ Carbonaro	Initial Release.	New guide to provide guidance for NIST SP 800-53, Revision 5, SR controls.	N/A
		Revision 1 - April 2, 2025		
1	Salamon/ Carbonaro/ Normand/ Peralta/ Klemens	Revisions included: • Updated control parameters to align with the Control Tailoring Workbook (CTW) and Common Control Catalog (CCC). • Added leading zeros to controls and updated implementation guidance to align with the CCC. • Moved CSF categories, Policy, References, and Roles and Responsibilities to Appendices.	Align to the latest GSA guidance.	Throughout
		Revision 2 - October 1, 2026		
1	Salamon/ Carbonaro/ Normand/ Peralta/ Klemens	Revisions included: • Added Section 3 on Defining Cyber Supply Chain Events and Incidents. • Updated control sections to align with revised baselines. • Added SR-04. • Updated mini tables throughout. • Updated Appendix A to CSF 2.0. • Updated Appendix B and D to align with the latest version of 2100.1.	Align to the latest GSA guidance.	Throughout

Approval

IT Security Procedural Guide: Supply Chain Risk Management (SR) controls, CIO-IT Security 22-120, Revision 2, is hereby approved for distribution.

DocuSigned by:

CABEEF810EDA7425

Joseph Hoyt
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Security Risk & Compliance Division (ISA), C-SCRM Program at 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	Defining Cyber Supply Chain Events and Incidents	2
4	GSA Implementation Guidance for SR Controls	4
4.1	SR-01 Policy and Procedures.....	5
4.2	SR-02 Supply Chain Risk Management Plan.....	6
4.3	SR-02(01) Supply Chain Risk Management Plan Establish SCRM Team.....	7
4.4	SR-03 Supply Chain Controls and Processes.....	8
4.5	SR-04 Provenance	9
4.6	SR-05 Acquisition Strategies, Tools, and Methods	10
4.7	SR-06 Supplier Assessments and Reviews.....	10
4.8	SR-08 Notification Agreements.....	11
4.9	SR-09 Tamper Resistance and Detection.....	12
4.10	SR-09(01) Tamper Resistance and Detection Multiple Stages of System Development Life Cycle	12
4.11	SR-10 Inspection of Systems or Components	13
4.12	SR-11 Component Authenticity.....	13
4.13	SR-11(01) Component Authenticity Anti-Counterfeit Training.....	14
4.14	SR-11(02) Component Authenticity Configuration Control for Component Service and Repair	15
4.15	SR-12 Component Disposal	15
5	Summary.....	16
	Appendix A: CSF Categories/Subcategories	17
	Appendix B: Policy	20
	Appendix C: References.....	21
	Appendix D: Roles and Responsibilities	22
	Appendix E: Definitions.....	25

List of Tables

Table 3-1. Designation of SR Controls	4
Table 3-2. Designation of SR Control Applicability	4
Table 3-3. Example Mini Table.....	5
Table A-1. CSF Functions/Categories and the SR Control Family.....	17
Table E-1. Definitions.....	25

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-r1-upd1, "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." The National Institute of Standards and Technology (NIST) has published The NIST Cybersecurity Framework 2.0 (CSF 2.0) as the latest version of the Framework. The 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](#).

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 Defining Cyber Supply Chain Events and Incidents

CIO-IT Security-01-02: Incident Response (IR) states, "An 'incident' or 'information security incident' is a violation or imminent threat of violation of information security or privacy policies, acceptable use policies, or standard security practices." Cyber supply chain incidents, in some cases, might become GSA IT security incidents.

The definition of a cyber supply chain event is one of the following related to a GSA ICT product or service that it uses for itself (not purchased on behalf of another agency):

1. Any notification that requires additional investigation to determine whether the Confidentiality, Integrity, and Availability of GSA data and information systems can be directly attributed to an attack involving the refurbishment, tampering, or counterfeiting of ICT products.
2. Any identified event that could significantly reduce confidence in cyber supply chain controls, such as the identification of ownership or governance related to restricted nations and their influence.
3. The presence of any of the prohibited sources outlined in GSA's [C-SCRM Policies, Regulations, and Laws: Prohibited Sources](#) InSite page including:
 - a. [Section 1634](#) of the "National Defense Authorization Act for Fiscal Year 2018."
 - i. Kaspersky Lab (or any successor entity).
 - ii. Any entity that controls, is controlled by, or is under common control with Kaspersky Lab.
 - iii. Any entity of which Kaspersky Lab has majority ownership.
 - b. [Section 889](#) of the "National Defense Authorization Act for Fiscal Year 2019"
 - i. Dahua Technology Company.
 - ii. Hangzhou Hikvision Digital Technology.
 - iii. Huawei Technologies Company.
 - iv. Hytera Communications Corporation.
 - v. ZTE Corporation.
 - c. Any subsidiaries or affiliates of the listed companies.
4. Vendors from the International Trade Administration [Consolidated Screening List](#) of entities that are banned from entering contracts with the government.

A cyber supply chain event can become a cyber supply chain incident under the following conditions:

1. An event which violates [GSA Order CIO 2100.1](#), "GSA Information Technology (IT) Security Policy."
2. A confirmed purchase made in violation of a law or regulation.

Note that supply chain events might never become supply chain incidents but may pose a risk that would require remediation.

The C-SCRM Program considers any evidence of suspicious Foreign Ownership, Control, and Influence (FOCI) as it can result in any of the above incidents. Evidence of such should be considered an event until confirmed as an incident.

Examples of potential cyber supply chain incidents or events can occur within the following areas:

- ICT Supplier infrastructure
 - Product development environment
 - 3rd party component Integrator
- Vendor infrastructure
 - Distribution center (physical security)
 - IT environment

- Customer intervention
 - (Intentional or accidental) compromise
- Refurbishment center
- Substitution

4 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-06
Moderate	SR-04, SR-06
High	SR-03, SR-04, SR-06, SR-09, SR-09(01), SR-11, SR-11(01), SR-11(02), SR-12
MiSaaS	SR-06

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. A few controls in the following sections are identified as C/H for Federal systems with additional information provided for each control.

Table 3-3. Example Mini Table

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

4.1 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 [\[review annually and update as necessary\]](#) and following [\[changes to Federal or GSA policies, requirements, or guidance\]](#); and
 2. Procedures [\[at least every three \(3\) years\]](#) and following [\[changes to Federal or GSA policies, requirements, or guidance\]](#).

	CCC	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. Supply Chain Risk Management policies in CIO 2100.1 as necessary after an annual review, and following relevant changes to Federal or GSA policies, requirements, or guidance.
2. CIO-IT Security-22-120 every three years and following relevant 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.

4.2 SR-02 Supply Chain Risk Management Plan

- 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: [\[all systems, system components, or system services unless explicitly excluded and approved by the GSA CISO and AO\]](#);
- Review and update the supply chain risk management plan [\[every 3 years\]](#) or as required, to address threat, organizational or environmental changes; and
- Protect the supply chain risk management plan from unauthorized disclosure and modification.

	CCC	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 in the "OCISO Cyber Supply Chain Risk Management (C-SCRM) Program Standard Operating Procedure (SOP)." The SOP serves as the Tier 2 (organizational) plan for GSA IT consistent with NIST SP 800-161. It identifies how the OCISO C-SCRM Program within the Security Risk and Management Division (ISA) 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 additional SOPs that detail how the program activities are executed.

ISA ensures the OCISO C-SCRM Program SOP is updated at least every 3 years. ISA SOPs are stored within Google Shared Drives that have restricted access.

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. As identified by NIST SP 800-161, organizations can develop Tier 2 plans that are inherited by systems within their control. A System Security Plan (SSP) 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. An SSP can serve as a Tier 3 plan for any organization with a Tier 2 plan.

4.3 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](#)].

	CCC	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 Security Risk & Compliance Division (ISA) 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 800-161r1-upd1.

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.

4.4 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].

	CCC	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 SSP 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’ SSPs 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 800-161r1-upd1. Each Vendor/Contractor owned/operated system is required to align its SSP security control requirements with NIST 800-53 security control selections as detailed in the GSA CTW.

4.5 SR-04 Provenance

Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: [all agency-owned, agency-operated, agency-authorized, or agency-managed systems and services, and all software, source code, scripts, configurations, infrastructure-as-code, packages, dependencies, containers, build artifacts, and third-party components developed, acquired, deployed, executed, or maintained by or on behalf of the agency, including associated provenance, integrity, supplier, dependency, build, approval, and deployment metadata].

	CCC	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
SR-04			✓	✓			S	S

GSA Implementation Guidance

Each system must document, monitor, and maintain valid provenance for agency systems, services, software, source code, scripts, configurations, infrastructure-as-code, packages, dependencies, containers, build artifacts, and third-party components throughout their lifecycle. This guidance applies to all agency-owned, agency-operated, agency-authorized, or agency-managed systems and services, including those developed, acquired, deployed, executed, or maintained by or on behalf of the agency.

Example control implementation statement for COTS provenance:

[System Name] documents and maintains COTS software provenance by recording supplier, acquisition, version, integrity, approval, deployment, and maintenance information in approved systems. COTS products are obtained from approved sources, validated using signatures, hashes, malware scans, or vendor documentation where available, and stored in controlled repositories.

Deployments are linked to approved change records and tracked through asset, configuration, and endpoint management tools. COTS products are monitored for vulnerabilities, vendor advisories, support status, and unauthorized version changes, with exceptions documented, approved, and periodically reviewed.

Federal System-Specific Expectation

System Owners must document and maintain provenance for managed systems, services, software, source code, scripts, configurations, infrastructure-as-code, packages, dependencies, containers, build artifacts, and third-party components. Provenance metadata is captured through approved repositories, build pipelines, artifact registries, configuration management tools, asset inventories, and supplier records. Software Composition Analysis (SCA) tooling can be used, where applicable, to identify and track open-source and third-party components, dependency relationships, versions, licenses, known vulnerabilities, and associated risk or remediation status.

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. Each Vendor/Contractor owned/operated system is required to align its SSP security control requirements with NIST 800-53 security control selections as detailed in the GSA CTW.

4.6 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](#)].

	CCC	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 800-161r1-upd1.

4.7 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](#)].

	CCC	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 800-161r1-upd1.

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.

4.8 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 [\[notification of supply chain compromises; results of assessments or audits\]](#).

	CCC	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.

Vendor/Contractor System-Specific Expectation

Vendors/Contractors must establish system-specific or organization-wide Notification Agreements and procedures consistent with NIST SP 800-161r1-upd1.

4.9 SR-09 Tamper Resistance and Detection

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

	CCC	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.

4.10 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.

	CCC	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.

4.11 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)].

	CCC	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 800-161r1-upd1.

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.

4.12 SR-11 Component Authenticity

- a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and
- b. 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].

	CCC	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 800-161r1-upd1.

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.

4.13 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).

	CCC	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 800-161r1-upd1.

4.14 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: [\[all components\]](#).

	CCC	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.

4.15 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: [\[as described in the Media Protection procedural guide or Contractor recommendation as approved by the GSA CIO and AO\]](#).

	CCC	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: Media Protection (MP) when preparing their procedures, techniques, and methods.

5 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, ISA Division for guidance, at ispcompliance@gsa.gov.

Appendix A: CSF Categories/Subcategories

The CSF provides guidance to organizations to manage cybersecurity risks. Its use can help organizations to better understand, assess, prioritize, and communicate its cybersecurity efforts. The core of the CSF consists of six concurrent and continuous or readily responsive Functions:

Govern (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

Identify (ID): The organization's current cybersecurity risks are understood.

Protect (PR): Safeguards to manage the organization's cybersecurity risks are used.

Detect (DE): Possible cybersecurity attacks and compromises are found and analyzed.

Respond (RS): Actions regarding a detected cybersecurity incident are taken.

Recover (RC): Assets and operations affected by a cybersecurity incident are restored.

The GSA uses the CSF to complement its risk management process and cybersecurity program. The 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" as its foundation for managing system risk. More detailed information on how the CSF relates to GSA's use of the NIST RMF is contained in GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk.

Table A-1 lists the Categories and Subcategories from the CSF that are identified as related to the implementation of policies, procedures, and processes regarding the NIST SP 800-53 controls documented in this guide.

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

CSF Function	Subcategory/Description
GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered (SR-03, SR-05, SR-06, SR-08)
	GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated (SR-05)
	GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders (SR-02)
	GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes (SR-02)
	GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated (SR-02)
	GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced (SR-01)
	GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced

CSF Function	Subcategory/Description
	to reflect changes in requirements, threats, technology, and organizational mission (SR-01) GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction (SR-01, SR-06) GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks (SR-06) GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed (SR-06) GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders (SR-02, SR-03) GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally (SR-02, SR-03, SR-05) GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes (SR-01, SR-02, SR-03) GV.SC-04: Suppliers are known and prioritized by criticality (SR-06) GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties (SR-03, SR-05, SR-06, SR-10) GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships (SR-05, SR-06) GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship (SR-03, SR-06) GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities (SR-02, SR-03, SR-08) GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle (SR-02, SR-03, SR-05, SR-06) GV.SC-10: Cybersecurity supply chain risk

CSF Function	Subcategory/Description
	management plans include provisions for activities that occur after the conclusion of a partnership or service agreement (SR-02, SR-03, SR-05, SR-06)
IDENTIFY (ID): The organization's current cybersecurity risks are understood.	ID.AM-04: Inventories of services provided by suppliers are maintained (SR-02) ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles (SR-05, SR-12) ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use (SR-05, SR-06, SR-10, SR-11) ID.RA-10: Critical suppliers are assessed prior to acquisition (SR-06) ID.IM-01: Improvements are identified from evaluations (SR-01, SR-05) ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties (SR-01, SR-05) ID.IM-03: Improvements are identified from execution of operational processes, procedures, and activities (SR-01, SR-05) ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved (SR-02)
RESPOND (RS): Actions regarding a detected cybersecurity incident are taken	RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared (SR-03, SR-08) RS.CO-02: Internal and external stakeholders are notified of incidents (SR-03, SR-08) RS.CO-03: Information is shared with designated internal and external stakeholders (SR-03, SR-08)
RECOVER (RC): Assets and operations affected by a cybersecurity incident are restored	RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders (SR-08)

Appendix B: Policy

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

Policy Section 3.6, Cybersecurity Supply Chain Risk Management states:

This section identifies how the GSA's C-SCRM processes have been established, and are managed, monitored, and improved in accordance with the CSF 2.0 Govern Function. Additional information is provided on the GSA's internal C-SCRM Policies, Regulations, and Laws web page.

Note: Items identified as [Deleted] below are documents that have been deprecated. The next update to the policy will remove them from it.

- a. The following documents establish the GSA's C-SCRM strategy, program, policy, processes, and define supply chain roles and responsibilities. They are communicated by publishing them to internal and external websites. A quarterly email of updated security documents is distributed when they have been updated.
 - (1) This Order;
 - (2) [Deleted]; and
 - (3) GSA CIO-IT Security-22-120: Supply Chain Risk Management (SR) Controls.
- b. The following documents identify how C-SCRM is integrated into overall cybersecurity and enterprise risk management and how suppliers are identified and prioritized.
 - (1) GSA CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC);
 - (2) [Deleted]; and
 - (3) GSA CIO-IT Security-22-120: Supply Chain Risk Management (SR) Controls.
- c. The following documents establish the GSA's roles, responsibilities, and processes for C-SCRM requirements and reducing risks before entering into contracts or relationships with suppliers or third parties.
 - (1) [Deleted];
 - (2) GSA CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisitions; and
 - (3) General Services Acquisition Manual.
- d. The following guides describe the GSA's processes and procedures for assessing, responding to, and monitoring C-SCRM risks through their lifecycle including post contract or agreement. These guides also describe requirements for anti-counterfeit procedures, incident notification, response, and recovery regarding suppliers and third parties.
 - (1) GSA CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC);
 - (2) [Deleted]; and
 - (3) GSA CIO-IT Security-22-120: Supply Chain Risk Management (SR) Controls.

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 Cybersecurity Framework \(CSF\) 2.0](#), 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 800-161r1-upd1](#), 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 only available on the internal GSA InSite [IT Security Procedural Guides](#) page.

- CIO-IT Security-01-02: Incident Response (IR)
- CIO-IT Security-09-44: Plans of Action & Milestones (POA&M)
- CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC)

The following guides are available on the [GSA.gov IT Security Procedural Guides](#) webpage.

- 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

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)

The FISMA establishes the designation of a Senior Agency Information Security Officer by the CIO. 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, including SR 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;
- 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: Plan of Actions and Milestones (POA&M).

Information System Security Officers (ISSOs)

ISSOs are responsible for ensuring implementation of adequate system security and privacy protections, including proper control implementations, in order to manage cybersecurity risk.. Responsibilities include:

- Ensuring the system is operated, used, maintained, and disposed of IAW documented security policies and procedures. Necessary security controls, including SR 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;
- Developing POA&Ms regarding SR controls for all systems under their purview.

Information System Security Managers (ISSMs)

ISSMs are responsible for all IT system security and privacy matters for the systems under their authority. 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, including the implementation of SR controls.

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: Security and Privacy Requirements for IT Acquisition Efforts. 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 new solicitations for all GSA IT systems include the security contract language from GSA CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts.

Appendix E: Definitions

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

Table E-1. Definitions

Term	Definition
Risk (NIST Glossary)	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 (NIST Glossary)	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 (NIST Glossary)	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) (GSAM Definitions)	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 (NIST Glossary)	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 (GSAM Definitions)	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 (CIO 2100.1)	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) (CIO 2100.1)	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.