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

Initial Release

April 14, 2022

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

Approval

IT Security Procedural Guide: Supply Chain Risk Management (SR) Controls, CIO-IT Security 22-120, Initial Release is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD7179261615 44F...

Bo Berlas
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

Table of Contents

List of Tables

Notes:

- 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 Section 1.4.
- It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

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 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 Systems Security Officer (ISSO) through the appropriate Information Systems 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).

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 1-1, 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[1]. 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 1-1 CSF Categories/Subcategories and the SR Control Family

CSF Category/Subcategory Identifier	Definition/Description
Business Environment (ID.BE): 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.	**ID.BE-1:** The organization's role in the cyber supply chain is identified and communicated. SR-1, SR-3 **ID.BE-4:** Dependencies and critical functions for delivery of critical services are established. SR-2
Governance (ID.GV): 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.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated. SR-1 **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. SR-1
Supply Chain Risk Management (ID.SC): 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.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders. SR-1, SR-2, SR-3, SR-5 **ID.SC-2:** 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-2, SR-3, SR-5, SR-6 **ID.SC-3:** 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-2, SR-3, SR-5
Information Protection Processes and Procedures	**PR.IP-6:** Data is destroyed according to policy. SR-12

[1] Mappings derived from: https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/csf-pf-to-sp800-53r5-mappings.xlsx

CSF Category/Subcategory Identifier	Definition/Description
(PR.IP): 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.	
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-2:** Detection activities comply with all applicable requirements SR-1, SR-9, SR-10
Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-5:** 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-6

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 information 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 information 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 information system is an information system:

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

1.3 Policy

CIO 2100.1 contains the following policy statements regarding C-SCRM.

Chapter 3, Policy for Identify Function

2. <u>Business Environment.</u>

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.

Note: The policy statements below were established before NIST SP 800-53, Revision 5 was published. An update to CIO 2100.1 is in process for incorporating the changes in Revision 5 making SR controls applicable based on FIPS levels.

a. *All FIPS 199 High Impact systems must manage risks to their supply chain IAW [in accordance with] NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations.*
b. *All FIPS 199 High Impact systems must, as part of supply chain risk management, assess the supply chain risk from suppliers and third-party partners.*
c. *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.*
d. *Systems and their suppliers and third-party suppliers must comply with Section 1634 of Public Law 115-91 that 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.*
e. *Systems and their suppliers and third-party partners must comply with 52.204-25 of the Federal Acquisition Regulation (FAR). It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232), the procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception or waiver is granted per the law or the FAR. Covered telecommunications equipment or services produced or provided by the following are prohibited: (1) Huawei Technologies Company (2) ZTE Corporation (3) Hytera Communications Corporation (4) Hangzhou Hikvision Digital Technology Company (5) Dahua Technology Company (6) Any subsidiary or affiliate of (1)-(5), above.*
f. *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.*
g. *All FIPS 199 High impact systems must incorporate Supply Chain Risk Management into response/recovery planning and testing IAW GSA CIO-IT Security-06- 29*

1.4 References

Federal Laws, Standards, Regulations, and Publications:

- EO 13800, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"
- EO 14028, "Executive Order 14028: Improving the Nation's Cybersecurity"
- 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 (Draft), "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-18-90 which is restricted. It is available on the internal 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-18-90, "Information Security Program Plan (ISPP)"
- CIO-IT Security-18-91, "Risk Management Strategy (RMS)"
- CIO-IT Security-21-117, "Cyber Supply Chain Risk Management OCISO (C-SCRM) Program"

2 Roles and Responsibilities

The System Program Managers/Project Managers 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.

2.1 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;

2.2 Federal Acquisition Service (FAS) Commissioner

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

2.3 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.

2.4 Authorizing Officials (AOs)

Authorizing Officials are the officials with the authority to formally assume responsibility for operating an information 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 information systems and issuing Authorization to Operate (ATO) approvals for each information system under their purview based on the acceptability of the security safeguards of the system (risk-management approach);
- Ensuring that GSA information 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.

2.5 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.

2.6 Information Systems 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.

2.7 Information Systems 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.

2.8 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.

2.9 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.

3 GSA Implementation Guidance for SR Controls

The GSA-defined parameter settings included in the control requirements are in blue, italicized 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 information systems and data. The GSA implementation guidance stated for each control applies to personnel and/or the information systems operated on behalf of 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-18-90, the ISPP, describes the GSA enterprise-wide common and hybrid controls and designates the responsible parties for implementing them.

Note: Until the ISPP is updated to NIST SP 800-53, Revision 5, contact ispcompliance@gsa.gov for guidance if there is a discrepancy between this guide and the ISPP.

Table 2-1 Designation of SR Controls

System Type	Federal	Contractor
Common	SR-1, SR-5, SR-8	
Hybrid	SR-2, SR-2(1), SR-3, SR-6, SR-11, SR-11(1)	SR-1
System-Specific	SR-9, SR-9(1), SR-10, SR-11(2), SR-12	SR-2, SR-2(1), SR-3, SR-5, SR-6, SR-8, SR-9, SR-9(1), SR-10, SR-11, SR-11(1), SR-11(2), 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-1, SR-2, SR-2(1), SR-3, SR-5, SR-8, SR-10, SR-11, SR-11(1), SR-11(2), SR-12
Moderate	SR-1, SR-2, SR-2(1), SR-3, SR-5, SR-6, SR-8, SR-10, SR-11, SR-11(1), SR-11(2), SR-12
High	SR-1, SR-2, SR-2(1), SR-3, SR-5, SR-6, SR-8, SR-9, SR-9(1), SR-10, SR-11, SR-11(1), SR-11(2), SR-12

3.1 SR-1: 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, GSA IT Security Policy*] 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*].

GSA Implementation Guidance: Control SR-1 is applicable at all FIPS 199 levels. NIST's SR-1 is a Common Control for Federal systems and a Hybrid Control for Contractor systems.

Common Control Implementation: The GSA SCRM policy is defined in CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding SCRM for GSA systems. 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 website.

The SCRM procedures are documented in CIO-IT Security-22-120, "IT Security Procedural Guide: Supply Chain Risk Management (SR) Controls" [this guide]. The procedures facilitate the implementation of the SCRM policy and associated controls. The guide is disseminated GSA-wide via GSA's InSite centralized agency website.

Per CIO 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides. The GSA OCISO is responsible for reviewing and updating CIO 2100.1 annually. The GSA OCISO is responsible for reviewing and updating CIO-IT Security-10-50 every three years and following changes to Federal or GSA policies, requirements, or guidance.

Federal System System-Specific Expectation: None, SR-1 is a common control. SCRM Policy is included in CIO 2100.1, Chapter 3, Policy for Identity Function. The policy states, "systems must manage risks to their supply chain IAW NIST SP 800-161, SCRM Practices for Federal Information Systems and Organizations." However, GSA Services/Staff Offices (S/SO) or System Owners may augment the SCRM policies and procedures included in 2100.1 and CIO-IT Security-22-120 to address additional organizational or system-specific SCRM requirements. Any such policies and procedures must include established timeframes for updating them.

Additional Contractor System Considerations: Vendors/contractors are required to comply with GSA's policy and procedural guidance regarding SCRM, they may supplement (but not lessen) GSA's SCRM policy and procedures with the approval of the AO and CISO.

Note: Contractor systems, per CIO 2100.1, are information systems in GSA's inventory processing or containing GSA or Federal data where the infrastructure and applications are wholly operated, administered, managed, and maintained by a contractor in non-GSA facilities.

3.2 SR-2: 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 [*annually*] or as required, to address threat, organizational or environmental changes; and
c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

GSA Implementation Guidance: Control SR-2 is applicable at all FIPS 199 levels. SR-2 is a Hybrid Control with each system's respective Service Staff Office's or Responsible IT Organization's SCRM Plan for Federal systems. For Contractor systems, Control SR-2 is a System Specific Control and may align with their corporation or company's SCRM Plan.

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.

Federal System System-Specific Expectation: Systems identify their respective Service Staff Office's SCRM Plan, Responsible IT Organization's SCRM Plan, or their specific organization's SCRM Plan which they align to.

Additional Contractor System Considerations: Vendor/contractor owned/operated systems must have their own system specific SCRM Plan that detail response activities and reporting requirements to GSA consistent with NIST SP 800-161.

3.3 SR-2(1): 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 S/SO or Contractor recommended personnel, roles, and responsibilities as approved by the GSA CISO and AOs*] 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*].

GSA Implementation Guidance: Control SR-2(1) is applicable at all FIPS 199 levels. SR-2(1) is a Hybrid Control with each system's respective Service Staff Office's SCRM Plan or Responsible IT Organization's SCRM Plan for Federal systems. For Contractor systems, Control SR-2 (1) is a System Specific Control and may align with their corporation or company's SCRM Plan.

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.

Federal System System-Specific Expectation: Systems identify the respective Service Staff Office's SCRM Plan, Responsible IT Organization's SCRM Plan, or their specific organization's SCRM Plan to which they align.

Additional Contractor System Considerations: Vendor/contractor owned/operated systems 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-3: 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 [Control Tailoring Workbook]*]; and

c. Document the selected and implemented supply chain processes and controls in [*security and privacy plans*]

GSA Implementation Guidance: Control SR-3 is applicable at all FIPS 199 levels. SR-3 is a Hybrid Control with each system's respective Service Staff Office's SCRM Plan or Responsible IT Organization's SCRM Plan for Federal systems, and SR-3 is a System-Specific Control for Contractor systems.

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.

Federal System System-Specific Expectation: Systems identify their respective Service 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.

Additional Contractor System Considerations: 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.

3.5 SR-5: 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*].

GSA Implementation Guidance: Control SR-5 is applicable at all FIPS 199 levels. SR-5 is a Common Control for Federal systems and a System-Specific Control for Contractor systems.

Federal System Common Control Implementation: Acquisition requirements are defined for GSA purchase in the GSAM, consistent with Federal Acquisition Regulations. These are defined by the SCRM SAO and SCRM Review Board and compiled at the following webpage.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements. Vendor/contractor owned/operated systems must employ their own system-specific Acquisition Strategies, Tools, and Methods consistent with NIST SP 800-161.

3.6 SR-6: 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*].

GSA Implementation Guidance: Control SR-6 is applicable at the FIPS 199 Moderate and High levels. SR-6 is a Hybrid for Federal systems and a System-Specific Control for Contractor systems.

Annually, the identified supporting 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.

Federal System System-Specific Expectation: Systems are to identify their respective Service Staff Office's SCRM Plan or Responsible IT Organization's SCRM Plan they align to.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements. Vendor/contractor owned/operated systems must perform their own system-specific Supplier Assessments and Reviews consistent with NIST SP 800-161.

3.7 SR-8: 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*]

GSA Implementation Guidance: Control SR-8 is applicable at all FIPS 199 levels. SR-8 is a Common control for Federal systems and a System-Specific Control for Contractor systems.

Federal System Common Control Implementation : GSAM-2021-G511 establishes requirements for reporting and handling of cyber supply chain events for GSA, including supply chain compromises. The 52.204-25 of the Federal Acquisition Regulation (FAR), which prohibits specific telecommunications equipment, also requires initial reporting of any prohibited equipment or services within one business day.

Additional Contractor System Considerations: Vendor/contractor owned/operated systems must establish their own system-specific Notification Agreements consistent with NIST SP 800-161.

3.8 SR-9: Tamper Resistance and Detection

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

GSA Implementation Guidance: Control SR-9 is applicable only for systems with High FIPS 199 levels. SR-9 is a System Specific Control for both Federal and Contractor systems.

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 System-Specific Expectation: System Owners ensure their systems comply with the control statements by defining which systems, system components, or system services must be tested for tampering and tampering resistance.

Additional Contractor System Considerations: 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.

3.9 SR-9(1) Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle

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

GSA Implementation Guidance: Control SR-9(1) is applicable only for systems with High FIPS 199 levels. SR-9(1) is a System-Specific Control for both Federal and Contractor systems.

Federal System System-Specific Expectation: System Owners ensure anti-tamper technologies, tools, and techniques are available for system developers and that they are used throughout the SDLC.

Additional Contractor System Considerations: 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 and CIO-IT Security-18-90.

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-2(1)*] to detect tampering: [*systems or system components as identified by the Supply Chain Risk Management Team as identified in SR-2(1)*].

GSA Implementation Guidance: Control SR-10 is applicable at all FIPS 199 levels. SR-10 is a System-Specific Control for both Federal and Contractor systems.

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.

Federal System System-Specific Expectation: Personnel responsible for handling or for the configuration of federal systems should utilize their training as outlined in SR-11(1). To inspect and identify any signs of tampering for system components.

Additional Contractor System Considerations: Vendor/contractor owned/operated systems must establish their own system-specific Inspection of Systems or Components policy and procedures consistent with NIST SP 800-161.

3.11 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-6 and GSAM-2021-G511, Contractor: Contracting Officer.*]

GSA Implementation Guidance: Control SR-11 is applicable at all FIPS 199 levels. SR-11 is a Hybrid Control for Federal systems and a System-Specific Control for Contractor systems.

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.

Federal System System-Specific Expectation: Systems are to identify their respective Service Staff Office's SCRM Plan, responsible IT Organization's SCRM Plan, or their specific organization's SCRM Plan to which they align.

Additional Contractor System Considerations: Vendor/contractor owned/operated systems must establish their own system-specific 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(1): Component Authenticity | Anti-Counterfeit Training

Train [*the SCRM Team as identified in SR-2(1) and personnel associated with installing hardware components for GSA systems annually and upon entry*] to detect counterfeit system components (including hardware, software, and firmware).

GSA Implementation Guidance: Control SR-11(1) is applicable at all FIPS 199 levels. SR-11(1) is a Hybrid Control for Federal systems and a System-Specific Control for Contractor systems.

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.

Federal System System-Specific Expectation: System Owners ensure SCRM Team members and personnel associated with installing hardware components follow counterfeit system component detection training consistent with NIST SP 800-161.

Additional Contractor System Considerations: Vendor/contractor owned/operated systems must perform system-specific Anti-Counterfeit Training consistent with NIST SP 800-161.

3.13 SR-11(2): 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*].

GSA Implementation Guidance: Control SR-11(2) is applicable at all FIPS 199 levels. SR-11(2) is a System-Specific Control for both Federal and Contractor systems.

Federal System 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.

Additional Contractor System Considerations: 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*].

GSA Implementation Guidance: Control SR-12 is applicable at all FIPS 199 levels and is a System Specific Control for both Federal and Contractor systems.

Federal System System-Specific Expectation: System Owners ensure system's data, documentation or system components are disposed of properly and in accordance with GSA's Media Protection procedure guide. 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.

Additional Contractor System Considerations: 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 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.

Appendix A Definitions

Table A-1 identifies terms and their definitions used in this guide.

Table A-4 Definitions

Term	Definition
Risk	A combination of the probability that a particular threat will exploit a particular vulnerability resulting in a particular harmful consequence
Risk Assessment	The process of identifying an acceptable level of risk (and associated cost) based on the planned or existing implementation of risk mitigation strategies
Risk Management	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	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	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	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	An information system in GSA's inventory processing or containing GSA or Federal data where the infrastructure and applications are wholly operated, administered, managed, and maintained by a contractor 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.