IT Security Procedural Guide: OCISO Cyber Supply Chain Risk Management (C-SCRM) Program CIO-IT Security-21-117

Revision 2

March 7, 2024

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 – June 18, 2021		
N/A	ISI	New guide created to address cyber supply chain risks.	Guide developed to address supply chain risks per NIST SP 800-161 and 800-53, Revision 5.	N/A
		Revision 1 – March 7, 2023		
1	Salamon/ Carbonaro/ Klemens	Changes include: • Updating email address for reporting C-SCRM incidents. • Adding monthly C-SCRM reports. • Adding GSAM case references regarding C-SCRM. • Updating references. • Edited and formatted to the latest guide style.	Scheduled update	Throughout
		Revision 2 – March 7, 2024		
1	Salamon/ Carbonaro/ Klemens/ McCormick	• Added Information Sharing and Reporting section. • Updated Pre-award section. • Updated references. • Edited and formatted to the latest guide formatting.	Scheduled update	Throughout

Approval

IT Security Procedural Guide: OCISO Cyber Supply Chain Risk Management (C-SCRM) Program, CIO-IT Security 21-117, Revision 2, is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD7117926161544F...

Bo Berlas
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

Notes: Hyperlinks in this guide are provided as follows:

- Section 5 - References. This section contains hyperlinks to Federal Regulations/Guidance and to GSA web pages containing GSA policies, guides, and forms/templates.
- In running text - Hyperlinks will be provided if they link to a location within this document (i.e., a different section or an appendix) and upon first appearance.

1 Introduction

The General Services Administration (GSA) Office of the Chief Information Security Officer (OCISO) through the OCISO Cyber Supply Chain Risk Management (C-SCRM) Program is charged with independently assessing both new and existing information and communications technology (ICT) product suppliers and services to manage supply chain risk. By increasing transparency into the supply chains of GSA product suppliers and utilizing cybersecurity skill sets, the OCISO C-SCRM Program creates mitigating supply chain security controls throughout the GSA environment. By integrating with the acquisition processes for GSA information technology (IT), supply chain risks based on C-SCRM evaluations of providers can be considered in procurement decisions and can prevent the award of contracts to product or IT service providers who pose an unacceptable level of risk to the organization.

The GSA OCISO C-SCRM Program has been established to provide a C-SCRM capability for GSA IT and the systems that it supports. This program capability includes policies, procedures, and operational functions. The program manages cybersecurity risk introduced by third-party products through the establishment of new capabilities and updates to existing processes. The scope of the program focuses on C-SCRM risks within GSA IT, as other Services and Staff Offices (SSOs) in GSA are developing their own programs.

Agency-wide governance for SCRM is led by the Office of Governmentwide Policy (OGP) as part of a SCRM Review Board, SCRM Strategy Working Group, and SCRM Executive Board. The OCISO C-SCRM Program provides support to the SCRM Review Board and SCRM Strategy Working Group and the CISO is a member of the SCRM Executive Board. The SCRM Review Board is responsible for handling supply chain events reported by contracting officers, including prohibited vendor disclosures. The SCRM Strategy Working Group provides recommendations to the SCRM Executive Board for agency-wide SCRM activities and funding.

1.1 Purpose

The purpose of this guide is to provide an overview detailing the establishment of a C-SCRM program within OCISO for GSA IT. In accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161, Revision 1, “Supply Chain Risk Management for Information Systems and Organizations,” this document serves as the Tier 2 (organizational) plan for GSA IT. The program monitors cyber supply chain risk for GSA IT and, when necessary, facilitates remediation efforts in the event of a supply chain security incident. In addition, third-party tools and techniques will be leveraged using risk-based approaches at the organizational level.

1.2 Scope

The OCISO C-SCRM program focuses on C-SCRM risks within GSA IT, as well as assisting and providing subject matter expertise and guidance to other SSOs of the agency when needed. C-SCRM risks include any GSA IT products or services acquired from a third-party vendor deemed critical to the mission/function of GSA. This program is managed by the OCISO Identity Credential, and Access Management (ICAM) Shared Service Division (ISI).

2 C-SCRM Program Overview

The OCISO C-SCRM Program is aimed at mitigating GSA's exposure to systemic security issues currently impacting a world-wide interconnected information and communications technology (ICT) supply chain. As stated in NIST SP 800-161, Revision 1, tools, techniques, and practices used as a result of supply chain risk assessments, "*may provide protections against unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors, and poor development practices throughout the system development life cycle.*"

Aiming to foster new mitigating security controls within the GSA environment, the OCISO C-SCRM Program encourages the improvement of security controls for its suppliers. Additional goals of this program include the ability to assess suppliers, the results of which could be shared for consideration by other Federal Agencies and Critical Infrastructure Sector environments via relationships with GSA-wide SCRM governance structures, as well as government-wide structures (e.g., the Federal Acquisitions Security Council [FASC]).

The resulting program areas enable new security monitoring capabilities within other OCISO programs such as incident response, software security testing, building device testing, and ICAM.

The following sections detail the scope for the OCISO C-SCRM program.

2.1 Provide Coordination, Oversight, and Analysis for C-SCRM Events and Incidents

The GSA OCISO has updated the CIO-IT Security-01-02: Incident Response (IR) guide and supporting processes to direct any cyber supply chain incidents to the OCISO C-SCRM Program at c-scrm@gsa.gov, who will assist the GSA IR Team with any response actions and coordinate reporting to the GSA-wide SCRM governance structures.

The OCISO C-SCRM program has defined the escalation procedures that will occur once an event is identified. This includes events identified through operational monitoring, open-source information, and anything referred to the team by a third-party, such as the GSA IR Team. The procedures address:

- How the C-SCRM program will coordinate with the GSA IR Team.
- When the C-SCRM program will escalate events beyond GSA IT.
- Which organizations will receive reporting of these escalations.

2.2 Establish C-SCRM Procedures

C-SCRM best practices must be implemented within GSA IT. This includes providing guidance at the policy and procedural levels for the implementation of C-SCRM controls at the system level as part of the Assessment and Authorization (A&A) process.

2.3 Facilitate Supplier Reviews

Supplier reviews are of critical importance to the effective management of third-party risks. The ability to proactively work with acquisition staff in the overall evaluation of potential suppliers is a key component of an effective C-SCRM program.

2.4 Identify Potential Supplier Threats

Effective point-in-time reviews of IT products and their manufacturers is critical to assessing potential cyber supply chain risks from both the suppliers, as well as their products to the GSA IT Environment. The identification of potential security gaps in these products could help identify areas for review as part of a continuous monitoring strategy.

2.5 Provide Continuous Monitoring for Cyber Supply Chain Threats

The dynamic nature of supply chains requires a continuous monitoring solution which enables GSA to assess risks as they may present themselves. Augmenting point-in-time supplier assessments with real-time monitoring abilities greatly enhances the effectiveness of a C-SCRM program.

2.6 Information Sharing and Reporting

Monthly C-SCRM summary reports, consisting of metrics related to supplier reviews, overall risk posture as reported by supplier illumination tools, and cyber supply chain events and incidents, are compiled and communicated to system stakeholders. These reports are summarized along with operational activities, compiled into quarterly reports, and briefed to executives for visibility and information-sharing.

3 Defining Cyber Supply Chain Events and Incidents

CIO-IT Security-01-02 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, and 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 may 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 C-SCRM Program Components

This section identifies the elements of the OCISO C-SCRM Program, including its structure, how C-SCRM events and incidents are handled, and details for in-place components related to component-level hardware device testing and third-party supplier reviews. The components below outline an acceptable level of C-SCRM risk appetite and tolerance. The program balances the use of risk-based approaches given limited resources, provides processes to mitigate C-SCRM risk to an acceptable level for C-SCRM events and incidents, and does not tolerate counterfeit, prohibited, or compromised components if found.

4.1 Program Structure

The OCISO C-SCRM Program consists of three main components: Pre-award, Post-award, and Ongoing C-SCRM Program Support, as shown in Figure 4-1.

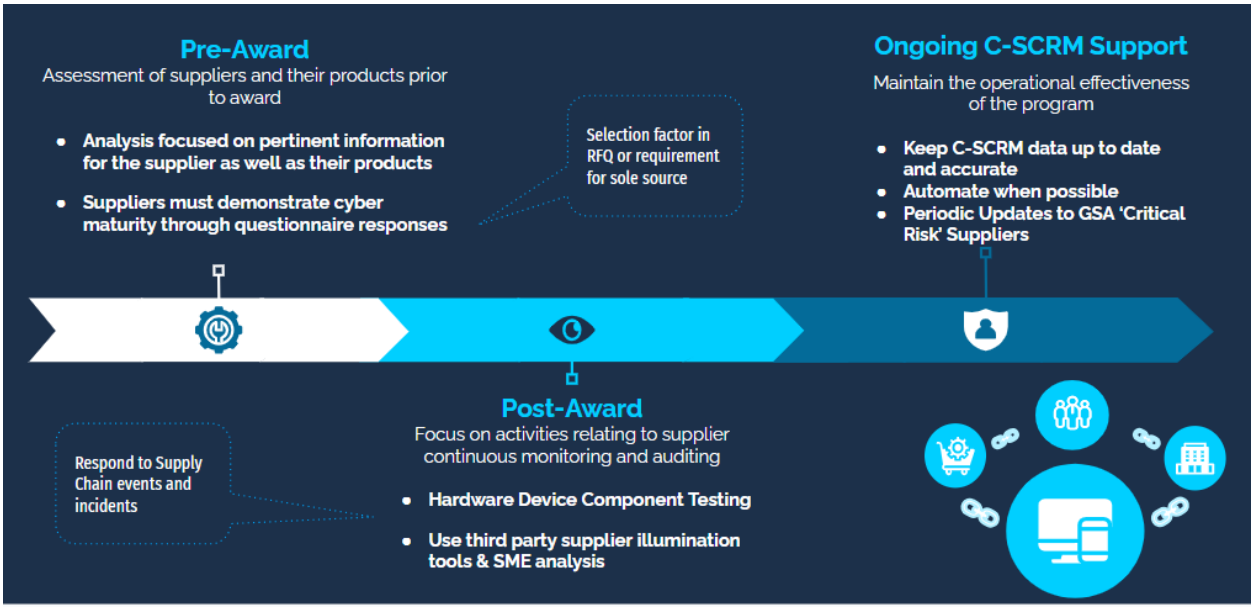

Figure 4-1. C-SCRM Program Structure

4.1.1 Pre-Award

The pre-award C-SCRM operations focus on reviewing original equipment manufacturers (OEM) ICT suppliers and their components prior to the award of acquisition contracts that meet certain criteria. This analysis focuses on the information pertinent to the supplier as well as their products.

Per a recent change to the GSA Acquisition Manual (GSAM 504.70), "Cyber-Supply Chain Risk Management," acquisition personnel must consider supply chain risk prior to acquisition if the product or service meets the criteria to be:

- GSA network-connected devices.
- Critical software.
- Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems," High or Moderate systems.

Additional pre-award components include:

- Reviewing credit card purchases made by the company in the event IT products are purchased outside the normal channels as described in the GSAM 504.70.
- Tracking IT product, service, and integrator suppliers who have already been reviewed.
- Reviewing non-buildings Internet of Things (IoT) devices for suitability for inclusion in GSA's IT Standards and compliance with H.R. 1668, "IoT Cybersecurity Improvement Act of 2020."

- Standardizing contract language for GSA IT acquisitions.

4.1.2 Post-Award

The post-award C-SCRM operations focuses on activities related to continuous monitoring and auditing of concurrent security practices of OEM suppliers and IT service providers to ensure cyber supply chain risks are continuously mitigated. This includes the following:

- Support for C-SCRM event and incident handling (detailed in Section 4.2).
- Component-level testing of hardware will also be conducted by third-party providers to identify instances of compromise (detailed in Section 4.3).
- Usage of third-party supplier illumination tools to supplement subject matter expert (SME) analysis (detailed in Section 4.4).

4.1.3 Ongoing C-SCRM Program Support

To provide and maintain an effective and up-to-date C-SCRM program, concurrent maintenance and security monitoring of critical risk suppliers is required. This also includes communication with identified suppliers to update any necessary and relevant information for the needs of the program.

4.2 C-SCRM Event and Incident Handling

The following identifies the responsibility of the GSA IR Team upon discovery of a possible Cyber SCRM event:

> *OCISO has established a Cyber Supply Chain Risk Management (C-SCRM) Program within the ICAM Shared Services Division (ISI). Any IT security incident that involves a potential compromise of the supply chain for any GSA system or data should be forwarded to c-scrm@gsa.gov. OCISO C-SCRM personnel will coordinate with the Incident Response Team and ensure that other entities within GSA or outside GSA are informed, as required.*

Upon receiving a communication regarding a possible C-SCRM event from any source, the C-SCRM personnel will review the information provided to determine if the criteria for a cyber supply chain event have been met. Pertinent event artifacts will be documented.

After notifying the OCISO C-SCRM Program contacts and gathering any needed additional information, a determination will be made whether the event should be declared a cyber supply chain incident and be handled as such. If the incident is also categorized as an IT security incident, the C-SCRM Program and GSA IR Team will work together in accordance with existing procedures documented in CIO-IT Security-01-02.

4.2.1 C-SCRM Event and Incident Reporting

If it is determined that a security event was caused by a vector to, or within the cyber supply chain, it must be categorized as a cyber supply chain incident. At the discretion of the OCISO C-SCRM Program, a “lessons learned” meeting will be conducted at the conclusion of a significant supply chain incident.

GSAM 504.70 establishes requirements for reporting and handling of cyber supply chain events and compromises for GSA. Should an individual suspect a cyber supply chain event has

occurred, the individual should contact the GSA Service Desk at itservicedesk@gsa.gov. The Service Desk will help determine if the event is a cyber supply chain event and contact the OCISO C-SCRM team to report the event if needed.

4.2.2 Criteria for Reporting Outside of Affected Organization

Sharing of pertinent information with stakeholders as part of ongoing supplier reviews or event investigations is an important aspect of a supply chain risk management program. Working with affected or potentially at-risk organizations can help mitigate impacts of supply chain incidents.

If it is determined a cyber supply chain incident involves a prohibited vendor, it will be reported to the GSA SCRM Review Board. Should a potential incident be reported from a GSA supplier, the C-SCRM Program shall ensure through direct communication with the reporting Contract Officer (CO) as outlined in How to Report an Issue (C-SCRM).

For any C-SCRM events that may have potential impact for other organizations, at the discretion of the ISI Director, events can be sent to GSA's other SCRM points of contact.

4.3 Component-Level Hardware Device Testing

Integrity testing on software and hardware components devices, to include IoT devices, is an important security control for an effective C-SCRM program. Sample tests of critical devices may help detect and potentially thwart attacks through the supply chain at an operational and ongoing level. The necessity for this capability is three-fold:

1. The capability to do so will allow the GSA to perform on-demand testing to identify evidence of device compromise.
2. Counterfeit detection controls are required for FIPS 199 Moderate and High impact systems as part of the new C-SCRM controls in NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations."
3. Prohibited vendors can also be identified by reviewing device components.

GSA uses a third-party service to conduct this testing. Devices from throughout the GSA IT organization are selected using a risk-based approach, prioritizing hardware such as:

- Components of buildings automation systems due to threat for real-world impact,
- Networking devices as they have visibility into large amounts of information, and
- Products adopted by the enterprise.

4.4 Third-Party Vendor Monitoring

As a part of the OCISO C-SCRM Program, a third-party service is used to augment existing controls to identify potential FOCI issues with the product supply chains. FOCI issues are complex issues and can pose a threat to GSA systems and data.

The use of a third-party vendor monitoring solution can identify:

- Legal and Regulatory Prohibited Vendor Violations
- Augmentation of Bill of Materials (BOM), if available
- Subsidiary and Acquisition Entity Tracking
- Cybersecurity risks

While the use of a third-party vendor monitoring solution is not a replacement for human gathered and verified intelligence, the means of providing supplemental value to a C-SCRM program as described in the use cases above is needed from a Defense-in-Depth cybersecurity approach and continuous monitoring standpoint.

A risk-based approach is used to identify which vendors are monitored to ensure no major changes have been made to the supplier's corporate or security infrastructure that could have major impacts on the security of the product. This includes changes to the geographical location of the value chain, such as development environments or factories, which may impact GSA IT products or services.

5 References

Note: GSA updates its IT security policies and procedural guides on independent cycles which may introduce conflicting guidance until revised guides are developed. In addition, some listed references are updated by external organizations which can lead to inconsistencies with GSA policies and guides. When conflicts or inconsistencies are noticed, please contact ispcompliance@gsa.gov for guidance.

Federal Laws, Regulations, and Guidance:

- H.R. 1668, "IoT Cybersecurity Improvement Act of 2020"
- H.R. 2810, "National Defense Authorization Act for Fiscal Year 2018"
- H.R. 5515, "National Defense Authorization Act for Fiscal Year 2019"
- International Trade Administration Consolidated Screening List
- NISTIR 8276, "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry"
- NIST SP 800-53 Revision 5, "Security and Privacy Controls for Information Systems and Organizations"
- NIST SP 800-16, Revision 1, "Cybersecurity Supply Chain Risk Management Practices for Information Systems and Organizations"

GSA Guidance:

- GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy"
- CIO-IT Security-01-02: Incident Response (IR)"
- GSA How to Report an Issue (C-SCRM) (Event Reporting Process)
- General Services Acquisition Manual, Subpart 504.70, "Cyber-Supply Chain Risk Management"
- GSA C-SCRM Policies, Regulations, and Laws: Prohibited Sources