

IT Security Procedural Guide:

OCISO Cyber Supply Chain Risk Management (C-SCRM) Program

CIO-IT Security-21-117

**Initial Release**

October 26, 2021

**VERSION HISTORY/CHANGE RECORD**

| **Change Number** | **Person Posting Change** | **Change** | **Reason for Change** | **Page Number of Change** |
| --- | --- | --- | --- | --- |
|  |  | **Initial Release – October 26, 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 |

**Approval**

IT Security Procedural Guide: OCISO C-SCRM Program, CIO-IT Security 21-117, Initial Release, is hereby approved for distribution.



**Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at ispcompliance@gsa.gov.**

Table of Contents

1 Introduction 2

1.1 Purpose 2

1.2 Scope 2

2 C-SCRM Program Overview 3

2.1 Provide Coordination, Oversight, and Analysis for C-SCRM Events and Incidents 3

2.2 Establish C-SCRM Procedures 4

2.3 Facilitate Supplier Reviews 4

2.4 Identify Potential Supplier Threats 4

2.5 Provide Continuous Monitoring for Cyber Supply Chain Threats 4

3 Defining Cyber Supply Chain Events and Incidents 4

4 C-SCRM Program Components 6

4.1 Program Structure 6

4.1.1 Pre-Award 6

4.1.2 Post-Award 7

4.1.3 Ongoing C-SCRM Program Support 7

4.2 C-SCRM Event and Incident Handling 7

4.2.1 C-SCRM Event and Incident Reporting 7

4.2.2 Criteria for Reporting Outside of Affected Organization 8

4.3 Component-Level Hardware Device Testing 8

4.4 Third-Party Vendor Monitoring 8

5 References 9

[Figure 4-1 – C SCRM Program Structure 6](#_Toc74815948)

**Notes:**

* 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). Hyperlinks will be provided for external sources unless the hyperlink is to a webpage or document listed in [Section 5](#_References_1). For example, Google Forms, Google Docs, and websites will have links.
* 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.

# Introduction

It is intended that the General Services Administration (GSA) Office of the Chief Information Security Officer (OCISO) through the OCISO Cyber Supply Chain Risk Management (C-SCRM) Program will be able to independently assess both new and existing “intelligent” 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 will create mitigating supply chain security controls throughout the GSA environment. By integrating with the acquisition processes for GSA IT, supply chain risks can be considered in procurement decisions based on C-SCRM evaluations of providers; 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. This program capability includes policies, and procedures, and operational functions. This program manages cybersecurity risk introduced by third-party products through the establishment of new capabilities and updates to existing processes capabilities. The scope of this program will focus on C-SCRM risks within GSA IT, as other Services / Staff Offices 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.

## 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, “*Supply Chain Risk Management for Federal Information Systems and Organizations”*, this document serves as the Tier 2 (organizational) plan for GSA IT. The program will monitor cyber supply chain risk for GSA IT and, when necessary, facilitate 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.

## Scope

The scope of this program will focus on C-SCRM risks within GSA IT, as well as assisting and providing subject matter expertise and guidance to other portions 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 the agency. This program is managed by the OCISO Identity Credential, and Access Management (ICAM) Shared Service Division (ISI).

# 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 defined by NIST SP 800-161, these issues include, but are not limited to: “*insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the ICT supply chain.*”

Aiming to foster new mitigating security controls within the GSA environment, the OCISO C-SCRM Program will encourage the improvement of security controls for its suppliers. Additional goals of this program will be the ability to assess suppliers, 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 will enable new security monitoring capabilities within other OCISO programs such as incident response, software security testing, building device testing, and ICAM.

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

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

The GSA CISO has updated IT Security Procedural Guide CIO-01-02: Incident Response (IR) and supporting processes to direct any cyber supply chain incidents to the OCISO C-SCRM Program at isi-federal@gsa.gov, who will assist the GSA Incident Response 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 Incident Response Team. The procedures address:

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

## 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.

## 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.

## 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 in gaps in these products could help identify areas for review as part of a continuous monitoring strategy.

## Provide Continuous Monitoring for Cyber Supply Chain Threats

The dynamic nature of supplier value chains requires a continuous monitoring solution which will enable 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.

# Defining Cyber Supply Chain Events and Incidents

The definition of a cyber supply chain incident is described below. According to CIO-IT Security-01-02, an “*IT Security Incident*” can be defined as 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. Presence of any of the prohibited sources outlined in the [prohibited acquisition sources](https://insite.gsa.gov/employee-resources/acquisition-purchases-and-payments/acquisition-portal/acquisition-by-topic/prohibited-sources-and-supply-chain-risk-management-scrm) on Insite:
   1. Section 1634 of the FY 2018 National Defense Authorization Act (NDAA)
   2. Kaspersky Lab (or any successor entity)
   3. Any entity that controls, is controlled by, or is under common control with Kaspersky Lab
   4. Any entity of which Kaspersky Lab has majority ownership
   5. Section 889 of the FY 2019 National Defense Authorization Act (NDAA)
   6. Dahua Technology Company
   7. Hangzhou Hikvision Digital Technology
   8. Huawei Technologies Company
   9. Hytera Communications Corporation
   10. ZTE Corporation
4. Any subsidiaries or affiliates of the listed companies.
5. Vendors from the [Consolidated Screening List](https://legacy.export.gov/csl-search) 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. Confirmed that a purchase was 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 should expressly consider 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

# 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. In building this new program, the components below outline an acceptable level of C-SCRM risk appetite and tolerance. It 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.

## Program Structure

The OCISO C-SCRM Program will comprise three main components: Pre-award, Post-award, and Ongoing C-SCRM Program Support.

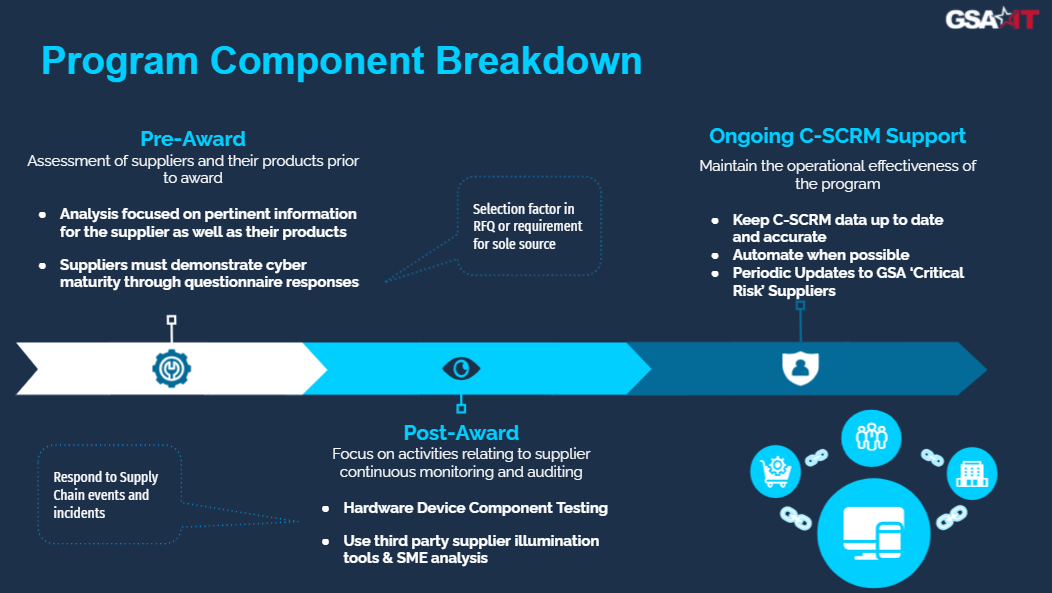


Figure 4- – C SCRM Program Structure

### Pre-Award

The pre-award C-SCRM operations will 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 will focus on the information pertinent to the supplier as well as their products. Pre-award components will include:

* Tracking of suppliers that have already been reviewed
* Pre-award supplier profiles and supporting questionnaires that may be part of a supplier review or incorporated into the acquisition.
* Standard contract language for GSA IT acquisitions

These components are not yet operationalized and will be targeted for piloting and expanded rollout.

### Post-Award

The post-award C-SCRM operations will focus 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)

### 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.

## C-SCRM Event and Incident Handling

The following identifies the responsibility of the GSA Incident Response 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 Program 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 Incident Response Team will work together in accordance with existing procedures documented in CIO-IT Security-01-02.

### 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.

### 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 the [GSA SCRM Event Reporting Process](https://insite.gsa.gov/employee-resources/acquisition-purchases-and-payments/acquisition-portal/acquisition-by-topic/prohibited-sources-and-scrm/scrm-event-report-process).

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.

## Component-Level Hardware Device Testing

Integrity testing on software and hardware components 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 detections controls are required for moderate impact systems as part of the new C-SCRM controls in NIST SP 800-53, Revision 5, “*Security and Privacy Controls For Information*.
3. Prohibited vendors can also be identified by reviewing device components

GSA uses a third-party service, the internal components of selected services as a service to the greater GSA organization. Devices from throughout the GSA IT organization are selected in a risk-based manner, prioritizing the following attributes:

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

## 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.

# References

**Note:** GSA updates its IT security policies and procedural guides on independent biennial cycles which may introduce conflicting guidance until revised guides are developed. In addition, many of the references listed 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. 2810](https://www.congress.gov/bill/115th-congress/house-bill/2810) – National Defense Authorization Act for Fiscal Year 2018
* [NISTIR 8276](https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf), “*Key Practices in Cyber Supply Chain Risk Management: Observations from Industry”*
* [NIST SP 800-53 Revision 5](https://doi.org/10.6028/NIST.SP.800-53r5), “*Security and Privacy Controls for Information Systems and Organizations”*
* [NIST SP 800-161](https://csrc.nist.gov/publications/detail/sp/800-161/final), “*Supply Chain Risk Management Practices for Federal Information Systems and Organizations”*

***GSA Guidance:***

* [GSA Order CIO 2100.1](https://insite.gsa.gov/directives-library/gsa-information-technology-it-security-policy-21001m-cio), “*GSA Information Technology (IT) Security Policy”*
* [GSA SCRM Event Report & Process](https://insite.gsa.gov/employee-resources/acquisition-purchases-and-payments/acquisition-portal/acquisition-by-topic/prohibited-sources-and-scrm/scrm-event-report-process)
* [Prohibited Sources and Supply Chain Risk Management (SCRM)](https://insite.gsa.gov/employee-resources/acquisition-purchases-and-payments/acquisition-portal/acquisition-by-topic/prohibited-sources-and-supply-chain-risk-management-scrm)

The guidance documents and template below are referenced within the body of this guide and are available on the GSA IT Security [Procedural Guides](https://insite.gsa.gov/employee-resources/information-technology/security-and-privacy/it-security/it-security-procedural-guides) and [Forms and Aids](https://insite.gsa.gov/employee-resources/information-technology/security-and-privacy/it-security/it-security-forms-and-aids) InSite pages.

* CIO-IT Security-01-02, “*Incident Response (IR)”*