DHS 4300A

Information Technology System Security Program

Sensitive Systems

Attachment D

Cybersecurity Supply Chain Risk Management (C-SCRM) Guidance

Version 1.2

July 22, 2022

This page intentionally blank.

Document Change History

Version	Date	Description
1.0	May 9, 2022	New Attachment – Cybersecurity Supply Chain Risk Management Dennis Martin
1.1	May 9, 2022	Technical Edit Review
1.2	July 22, 2022	OCISO Policy Edit Review, C Santangelo, incorporating Component CISO edits

TABLE OF CONTENTS

1.0 INTRODUCTION

This document guides the Department of Homeland Security (DHS) organization on the key C-SCRM tasks that need to be performed within DHS to ensure the security and integrity of the DHS Information and Communications Technology (ICT) supply chain.

2.0 SCOPE

This guidance applies to all ICT programs, products, and services within DHS that collect, generate, process, store, display, transmit, or receive For Official Use Only (FOUO), Sensitive But Unclassified (SBU), or any other unclassified information caveat that falls under the scope of the policy.

3.0 RESPONSIBILITIES

1. **Under Secretary for Management (USM)** reviews recommendations of the DHS CIO and the DHS Chief Acquisition Officer (CAO) regarding issuance of agency-level covered procurement actions, prior to submission to DHS Secretary.

2. **DHS Chief Information Officer (DHS CIO)** provides overall management, administration, oversight, and advises Components and the DHS Chief Information Security Officer (CISO) when implementing this guidance.
   (a) Establishes and maintains the DHS Cybersecurity Supply Chain Risk Management (C-SCRM) program to enable the risk owner(s) to identify, assess, and mitigate risks to the DHS ICT supply chain.
   (b) Establishes the DHS C-SCRM Program Management Office (C-SCRM PMO) with the mission and resources to assist in ensuring agency compliance with National Institute of Standards and Technology (NIST) C-SCRM requirements.
   (c) Develops, maintains, and evaluates the effectiveness of DHS C-SCRM policies, management controls, procedures, and practices based on standards and guidelines appropriate for the protection of in scope systems and information contained in such systems.
   (d) Influences and remains cognizant of new developments in C-SCRM issues, policies, and practices through consultation with the private sector and government agencies, including participation in the Federal CIO Council and NIST.
   (e) Issues joint recommendations with the Chief Acquisition Officer (CAO) to the Secretary for taking covered procurement actions.

3. **Component Chief Information Officers (CIOs)** implement this guidance within their organization and operations pursuant to governing laws, regulations, DHS C-SCRM directive, policy, and guidance.

4. **DHS Chief Information Security Officer (CISO)** ensures that all DHS Components comply with C-SCRM governing laws, regulations, this policy, and guidance, as well as other security measures required by statute, regulation, and policy.
   (a) Leads overall cross-enterprise coordination and collaboration with other applicable senior personnel within the enterprise, including the CAO, CIO, Chief Procurement

Officer (CPO), CFO, Executive Director of the Office of Program Accountability and Risk Management (PARM), the General Counsel (GC), and the risk executive (function).

(b) Coordination will be executed by the C-SCRM PMO and C-SCRM PMO working group (DHS C-SCRM WG).

(c) Participates in DHS Enterprise Risk Management (ERM) decision making council.

5. **Chief Procurement Officer (CPO)** ensures that programs and systems within their Component comply with governing laws, regulations, and this guidance.

Per delegation of the responsibilities of the DHS Chief Acquisition Officer [CAO]):

(a) Integrates DHS C-SCRM policy into DHS procurement processes and governance.

(b) Incorporates and enforces terms, conditions, and service level performance requirements into DHS supplier contracts to support DHS C-SCRM policy.

(c) In conjunction with the CIO, oversees the Department's acquisition program portfolio to monitor each investment's C-SCRM compliance.

(d) Issues joint recommendations with the CIO to the Secretary for taking covered procurement actions.

(e) Influences and remains cognizant of new developments in C-SCRM issues, policies, and practices through consultation with the private sector and government agencies, including participation in Federal acquisition bodies.

6. **DHS Chief Financial Officer (CFO)** integrates DHS C-SCRM policy into DHS financial management processes and governance.

(a) Develops C-SCRM practices for Purchase Card (P-Card) purchases of ICT that include the creation of ICT monitoring and reporting.

7. **DHS Executive Director of the DHS Office of Program Accountability and Risk Management (PARM)**:

(a) Ensures that C-SCRM is integrated in the acquisition life cycle process.

(b) Integrates DHS C-SCRM policy into DHS acquisition program management policy, procedures, and guidance processes.

(c) Monitors the C-SCRM PMO structure to assess adequacy of staffing compliance with Departmental policies and instructions.

(d) Advises and provides requirements to the Department Acquisition Career Manager (ACM) on certification standards for all acquisition program C-SCRM disciplines.

(e) Serves as the DHS executive agent, Acquisition Review Process coordinator, and Acquisition Review Board (ARB) Executive Secretariat with approval authority on selected C-SCRM acquisition program documentation.

8. **DHS Office of the General Counsel (OGC)**

(a) Advises the C-SCRM PMO regarding contract language to ensure accordance with all applicable statutes, regulations, and policies.

(b) Assesses policies and procedures and setting forth the legal standards for determining the legal sufficiency of C-SCRM signed documents.

(c) Reviews and concurs on the legal sufficiency of policy and guidance related to C-SCRM.

9. **DHS C-SCRM Program Management Office (PMO):** Dedicated office to support DHS Enterprise C-SCRM activities.

(a) Implements and oversees DHS C-SCRM policies, processes, and governance.

(b) Manages activities to identify, analyze, assess, and address risks to DHS Information and Communications Technology (ICT) supply chains.

(c) Establishes a DHS C-SCRM WG comprised of key DHS stakeholders for the purpose of guiding and informing C-SCRM policy and process, adjudicating C-SCRM issues and recommendations escalated by the C-SCRM PMO. Establishes C-SCRM tiger teams to address specific issues that require the expertise, authorities, and concurrence of other DHS stakeholders.

(d) Develops DHS Enterprise-level C-SCRM processes and procedures.

(e) For major DHS ICT acquisition programs, supports the Components and procurement/contracting offices in developing their own C-SCRM practices and programs for all contracting and acquisition actions and lifecycle management of systems.

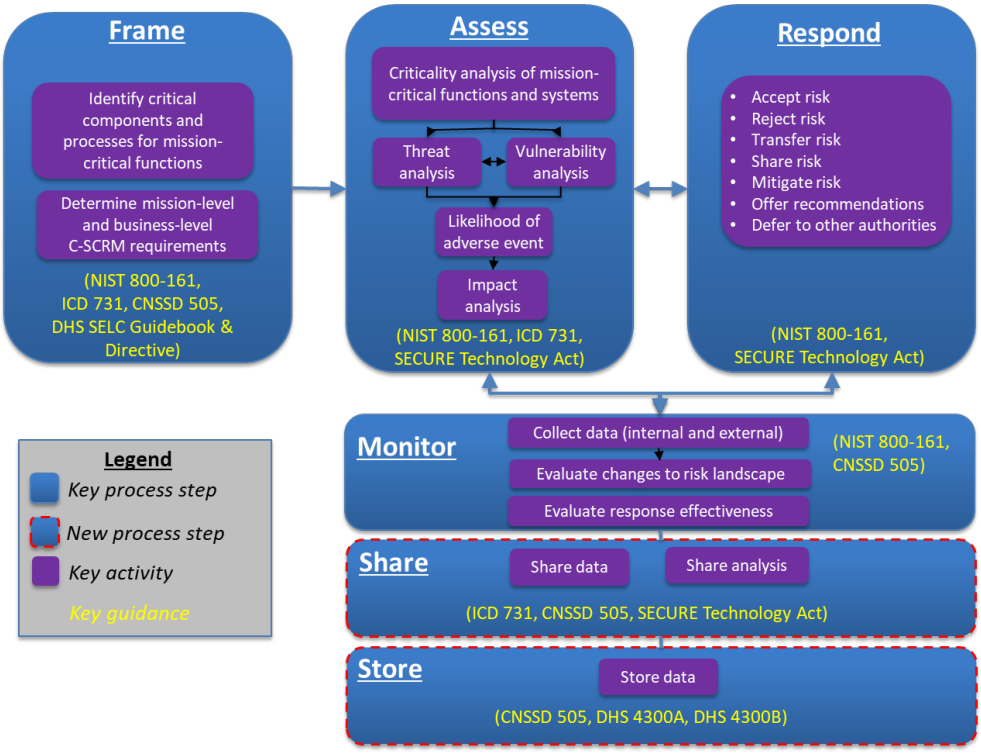
(f) For other ICT purchases, services, and products such as P-card ICT purchases, supports the Components and other DHS stakeholders in developing C-SCRM practices.

(g) Provides C-SCRM artifacts, such as document templates and job aids. Provides C-SCRM services such as vendor risk assessments.

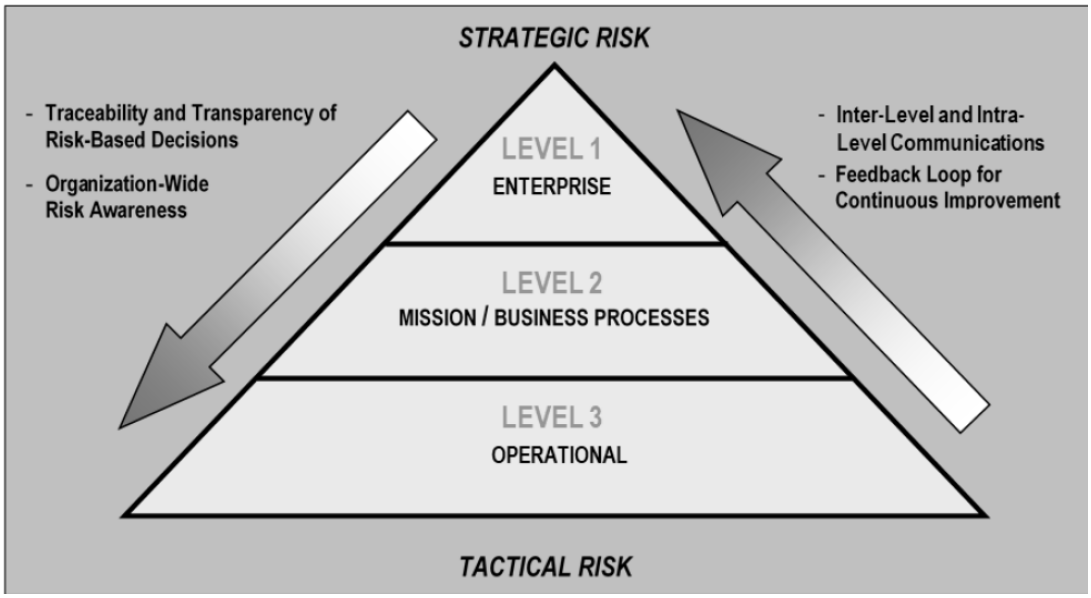
4.0 REQUIREMENTS

C-SCRM is to be integrated into DHS Enterprise-wide risk management process. Per NIST guidance, this process includes the following continuous and iterative steps:

- Frame risk - Establish the context for risk-based decisions and the current state of the Enterprise's information and communications technology and services and the associated supply chain.
- Assess risk - Review and interpret criticality, threat, vulnerability, likelihood, impact, and related information.
- Respond to risk - Select, tailor, and implement mitigation controls based on risk assessment findings.
- Monitor risk - Monitor risk exposure and the effectiveness of mitigating risk on an ongoing basis, including tracking changes to an information system or supply chain using effective Enterprise communications and a feedback loop for continuous improvement.



In addition, integration will address risk from different perspectives: 1) the Enterprise level, 2) the mission and business process level, and 3) the operational level. C-SCRM requires the involvement of all three levels.



Managing cybersecurity risks throughout the supply chain is a complex undertaking that requires DHS Components' collaboration.

5.0 PROCEDURES

Consistent with DHS C-SCRM guidance and policy promulgated by the C-SCRM PMO, DHS Components are responsible for implementing C-SCRM processes to all DHS ICT hardware and software components that can be exploited by an adversary or accidentally to degrade the capability of DHS to conduct its missions, or that could lead to the loss or destruction of DHS-sensitive data.

5.1 Level 1 – DHS Enterprise: DHS C-SCRM Strategy & Policy

Level 1 (DHS Enterprise) sets the tone and direction for DHS enterprise-wide C-SCRM activities by providing an overarching C-SCRM strategy, a C-SCRM policy, and a High-level Implementation Plan that shapes how C-SCRM is implemented across the enterprise.

Activities include:

- Define DHS C-SCRM strategy.
- Form governance structures and operating model.
- Form a DHS C-SCRM PMO.
- Frame risk for the Enterprise and set expectations for how risk is managed (e.g., set risk appetite).
- Define high-level implementation plan, policy, goals, and objectives. Develop DHS C-SCRM Strategic Implementation Plan.
- Make Enterprise-level C-SCRM Decisions.
- Conduct Cybersecurity Supply Chain Risk Assessments (C-SCRA) to review any third-party product, service, or supplier that could present a cybersecurity risk to a procurer.
- Adhere to the NIST-related SCRM controls as required by DHS Policy.

5.2 Level 2 – Mission and Business Process: DHS Components C-SCRM Strategies, Policies, & Plans

Level 2 addresses how the DHS Components' business processes assess, respond to, and monitor cybersecurity risks throughout the supply chain. Level 2 activities are performed in accordance with the C-SCRM strategy and policies provided by Level 1.

Activities include:

- Develop mission and business process-specific strategy.
- Develop C-SCRM strategic implementation plan(s).
- Develop policies and procedures, guidance, and constraints (DHS instructions).
- Reduce vulnerabilities at the onset of new IT projects and/or related acquisitions.
- Review and assess systemic, human, or organizational flaws that expose business, technical, and acquisition environments to cyber threats and attacks.
- Tailor the Enterprise risk framework to the mission and business process (e.g., set risk tolerances).
- Manage risk within mission and business processes.
- Establish a capability to manage C-SCRM responsibilities at the Component level.
- Collaborate with DHS C-SCRM PMO.
- Report progress on C-SCRM activities to Level 1
- Act on C-SCRM progress reporting from Level 3.

- Conduct Vendor Due Diligence Assessments (VDDAs) with templates provided by C-SCRM PMO.
- Adhere to the NIST-related SCRM controls as required by DHS Policy.

5.3 Level 3 – Operational: DHS Program and System Level C-SCRM Plans

Level 3 is comprised of personnel responsible and accountable for operational activities, including conducting procurements and executing system-related C-SCRM activities as part of the DHS Acquisition Lifecycle Framework (ALF) and Systems Engineering Life Cycle (SELC), which includes research and development, design, manufacturing, delivery, integration, operations and maintenance, and the disposal/retirement of systems. These personnel include system owners, contracting officers, contracting officer representatives, architects, system engineers, information security specialists, system integrators, and developers.

Activities include:

- Develop C-SCRM plans as part of Program or System Risk Management Plans.
- Implement C-SCRM policies, requirements, and controls for Programs and Systems.
- Adhere to constraints provided by Level 1 and Level 2.
- Tailor C-SCRM to the context of the individual program or system and apply it throughout the ALF and SELC.
- Report progress on C-SCRM activities to Level 2.
- Adhere to the NIST-related SCRM controls as required by DHS Policy.

6.0 AUTHORITIES/REFERENCES

A. NIST Special Publication NIST SP 800-161r1, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," May 2022.

B. NIST Special Publication 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View," March 2011

C. Public Law 107-347, "E-Government Act of 2002"

D. Public Law 113-283, "Federal Information Security Modernization Act (FISMA)"

E. Public Law 113.291, "Federal Information Technology Acquisition Reform Act (FITARA)"

F. Public Law 115-390, "SECURE Technology Act – Strengthening and enhancing Cyber-capabilities by utilizing Risk Exposure Technology"

G. Title II of Public Law 115-390, "Federal Acquisition Supply Chain Security Act (FASCSA)"

H. Public Law 116-283, "Section 889 National Defense Authorization Act for Fiscal Year 2019"

I. Title 44, United States Code (U.S.C.), Section 3544, "Federal Agency Responsibilities"

J. Executive Order (E.O.) 13526, "Classified National Security Information"

K. Executive Order (E.O.) 13636, "Improving Critical Infrastructure Cybersecurity"

L. Executive Order (E.O.) 13800, "Growing and Sustaining the Cybersecurity Workforce"

M. Executive Order (E.O.) 13833, "Enhancing the Effectiveness of Agency CIO"

N. Executive Order (E.O.) 13873, "Securing the Information and Communications Technologies and Services Supply Chain"

O. Executive Order (E.O.) 13913, "Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector"

P. Executive Order (E.O.) 14028, "Improving the Nation's Cybersecurity"

Q. Presidential Policy Directive PPD-8, "National Preparedness"

R. National Security Systems Directive 505, "Supply Chain Risk Management"

S. Intelligence Community Directive 731, "Supply Chain Risk Management"

T. OMB Circular A-130, "Managing Information as a Strategic Resource"

U. DHS Designation Number: 00-04004, "Designation of Chief Information Officer as Senior Agency Official for Supply Chain Risk Management"

V. DHS Delegation Number: 00701, "Delegation to the Chief Acquisition Officer"

7.0 Definitions

Covered telecommunications equipment and services means video surveillance and telecommunications equipment produced by certain technology companies defined (in accordance National Defense Authorization Act [NDAA] Pub. Law 116-283 Section 889).

Cybersecurity-Supply Chain Risk Management (C-SCRM) means a systematic process for managing exposures to cybersecurity risks, threats, and vulnerabilities throughout the supply chain and developing appropriate response strategies presented by the supplier, the supplied products, services, and the supply chain.

Information and Communication Technology (ICT) means the products and services that encompass the capture, storage, retrieval, processing, display, representation, presentation,

organization, management, security, transfer, and interchange of data and information. ICT includes networks; isolated Local Area Networks (LANs); standalone systems; and/or IT services; as well as applications for which DHS is responsible and has authority, regardless of the physical location.

Supply Chain Cybersecurity Risk Assessments is a systematic examination of cybersecurity risks throughout the supply chain, the likelihoods of their occurrence, and potential impacts.

Vendor Due Diligence Report (VDDA) is an open-source company Due Diligence Report (DDR) that provides an UNCLASSIFIED level DHS company risk tolerance control recommendation and a synopsis of the company C-SCRM findings to assist in various decisions regarding DHS hardware, software, and service deployment. It summarizes UNCLASSIFIED indicators of potential compromise of the specified company's information and communications technology and/or services (ICTS) supply chain. This report does not account for ICTS criticality to DHS missions, specific consequences to DHS missions due to compromise of the ICTS, nor does it account for potential classified threat reporting.