Draft NIST Special Publication 800-161 Revision 1

Cyber Supply Chain Risk Management Practices for Systems and Organizations

Jon Boyens
Angela Smith
Nadya Bartol
Kris Winkler
Alex Holbrook
Matthew Fallon

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-161r1-draft

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NIST Special Publication 800-161 Revision 1

Cyber Supply Chain Risk Management Practices for Systems and Organizations

Jon Boyens
Angela Smith
Computer Security Division
Information Technology Laboratory

Nadya Bartol
Kris Winkler
Alex Holbrook
Matthew Fallon
Boston Consulting Group

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-161r1-draft

April 2021

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-161 Revision 1
Natl. Inst. Stand. Technol. Spec. Publ. 800-161 Rev. 1, 277 pages (April 2021)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-161r1-draft

Public comment period: *April 29, 2021* through *June 14, 2021*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: scrm-nist@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

Organizations are concerned about the risks associated with products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable 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.

This publication provides guidance to organizations on identifying, assessing, and mitigating cyber supply chain risks at all levels of their organizations. The publication integrates cyber supply chain risk management (C-SCRM) into risk management activities by applying a multi-level, C-SCRM-specific approach, including guidance on development of C-SCRM strategy implementation plans, C-SCRM policies, C-SCRM plans, and C-SCRM risk assessments for products and services.

Keywords

C-SCRM; cyber supply chain risk management; acquire; information and communication technology; supply chain; cyber supply chain; supply chain assurance; supply chain risk; supply chain risk assessment; supply chain security; risk management; supplier.

Acknowledgements

The authors, Jon Boyens, National Institute of Standards and Technology (NIST), Angela Smith (NIST), Nadya Bartol, Boston Consulting Group (BCG), Kris Winkler (BCG), Alex Holbrook (BCG), and Matthew Fallon (BCG) would like to acknowledge and thank Celia Paulsen (NIST), and Rama Moorthy (Hatha Systems), the original authors of the NIST SP 800-161, Kelley Dempsey (NIST), Dr. Ron Ross (NIST), and Stephanie Shankles (U.S. Department of Veterans Affairs) for their contributions to and review of the original NIST SP 800-161. The authors would also like to thank the C-SCRM community, which has provided the authors invaluable insight and diverse perspectives to managing the cyber supply chain, especially the Departments and Agencies who provided us with their experience and documentation on NIST SP 800-161 implementation since its release in 2015.

Note to Reviewers

Revision 1 of this foundational NIST publication represents a one-year effort to incorporate the next generation C-SCRM controls that will be needed to accomplish the above objectives. It includes changes to make the SP more modular based, expand alignment to [NIST 800-37], *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* as well as NIST [800-39], *Managing Information Security Risk: Organization, Mission, and Information System View*. Changes also focus on making implementation guidance more consumable by acquirers, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers as well as increasing enablement through the inclusion of C-SCRM Strategy & Implementation Plan, C-SCRM Policy, C-SCRM Plan, and Cyber Supply Chain Risk Assessment templates.

Questions to reviewers:

- Does this document strike the right balance with respect to providing guidance any organization can use, regardless of size, mission, etc., and providing guidance sufficiently descriptive to be clear and actionable?
- Does this guidance offer organizations a structure both easy to follow and implement?? If not, how could the guidance be structured, the content be represented, and main points/concepts be highlighted so that the user can build a C-SCRM program and capabilities using the minimum amount of time and resources?
- Is anything missing in the implementation guidance that you would have expected to see? Is there any guidance that is not needed?
- Within Section 3.1.1 – Acquisition in the C-SCRM Strategy & Implementation Plan, are we providing the right balance of guidance?
- Within Section 3.4 – Is one implementation model preferred versus the other? Or both? Or is there a different approach preferred that is not currently reflected?
  Within Section 3.4.1 – Is the document providing the right balance and mix of capabilities across the Foundational, Sustaining, and Enhancing practice categories?
- Within Appendix D 4.1 Cyber Supply Chain Risk Assessment Template – What can improve the product or service assessment? Should it be combined with a supplier

assessment? What should be asked of the supplier? Should the assessment ask about the technology being acquired?

Major changes include:

- Updated diagrams and tables throughout

Additional major changes per section / appendix include:

Section 1, Introduction

- Refined cyber supply chain risk management definition to include internal and external dependency considerations to improve clarity.
- Clarified and expanded upon the meanings of the C-SCRM products, services (e.g., Human Resources, Payroll, Cloud Providers, and Managed Security), and supply chain elements.
- Incorporated types of factors that are associated with services that drive risk identification, assessment and response considerations.
- Described relationship between traditional supply chain (e.g., Supply Chain Operations Reference) and C-SCRM. Established NIST C-SCRM as the authoritative definition.
- Expanded scope from High Impact Systems to High, Moderate, and Low Impact Systems, per draft SP 800-53B (baselines); included Operational Technology (OT) and Internet of Things (IoT) considerations throughout.
- Added of *Section 1.3, The Business Case for C-SCRM*, and *Section 1.7 Implementing C-SCRM* in the context of SP 800-37 Rev. 2.
- Updated the regulatory, legislative, and guidance references to include developments since initial publication (e.g., SP 800-160, SP 800-53 Rev. 5, SECURE Technology Act of 2018, etc.).
- Acknowledgement of C-SCRM as a multidisciplinary topic that demands coordination across multiple disciplines (e.g., acquisition policy/management, logistics management, legal, and intelligence).
- Defined C-SCRM relational boundaries (e.g., National Security Systems, High Value Assets, Critical Infrastructure, and Government-as-Enterprise).

Section 2, Integration of C-SCRM into Organization-wide Risk Management

- Movement of Frame, Assess, Respond, Monitor (FARM) processes to Appendix C
- C-SCRM Program Management:
  - Defined the scope and characteristics of a C-SCRM Program across organizational tiers.
  - Introduced the concepts of a dedicated C-SCRM PMO within one or more organizational tiers and codify the C-SCRM PMO's purpose, high-level roles and responsibilities, and scope of responsibilities.
  - Explored models of vertical and horizontal coordination across organizational tiers, especially where numerous PMO responsibilities may overlap (e.g., facilitate matrix management and coordination of disparate discipline-area specific SCRM functions, enable governance and integration with enterprise risk

management, liaise with external entities/officials, track/manage/report on SCRM implementation progress and overall program effectiveness).
    - Consider resource and budgetary constraints via alternate operational models (e.g., formal and less formal PMOs), as well as methods for how to determine the model that is "fit for purpose".
    - Concrete guidance provided to assess and measure the effectiveness of an organization's C-SCRM program capabilities and program outcomes related to mitigating or otherwise appropriately managing cyber supply chain risks.
- Acquisition Security:
    - Acquisition Security concepts (further explored in Section 3) have been added across the risk framework levels.
    - Processes described from a Buyer's perspective (e.g., how a member of the Acquisition Team can effectively evaluate the relative merits of a given contractor's C-SCRM controls or their supply chain risk exposure and use that information appropriately when making acquisition-related decisions). Link to OMB A-123.
- Implementing C-SCRM in the Context of SP 800-37 Rev. 2:
    - Clear linkage made with SP 800-37 Rev 2. and System Level (Level 3) C-SCRM guidance.

This section included the following revisions:

- Risk Management Process:
    - Integrated into and enhanced existing frame, assess, respond, and monitor activities with the latest operational and technological trends. Improved traceability of tasks with their associated infographics. Generally, expanded roles and responsibilities concepts. Refined and clarified what risk tolerance means, who determines it and upon what it is based, and how it is used to inform and influence risk response decisions.
    - Discussed importance of a documented, foundational methodology that provides for a repeatable and standardized way to codify risk information via SP 800-37 Rev. 2 and the SP 800-53 Rev. 5 SR Family.
- Interdependencies:
    - Impact of external stakeholders, federated organizations, and other interdependencies on C-SCRM was reviewed and added to as necessary.

Section 3, (NEW) Critical success factors

Section 4, C-SCRM Controls – *previously section three*

- Updated all NIST SP 800-53 Rev. 4 mappings to NIST SP 800-53 Rev.
- Updated C-SCRM controls based on SP 800-53 Rev. 5. New control sets for SR (SR-13: Supplier Inventory) and MA (MA-8: Maintenance Monitoring and Information Sharing) were added:
    - Impact System Expansion - Designated which supplemental guidance is applicable to High, Moderate, and/or Low Impact Systems.

- Supplemental Guidance: Existing supplemental guidance was enhanced with the latest operational and technological trends, and implementation guidance was added per new or updated control language.

Appendix A – C-SCRM Control Summary

Appendix B – Risk Response Framework
- Changed title from Cyber Supply Chain Threat Events to Risk Response Framework.
- Updated language to incorporate risk-based approach.
- Added Scenario 1.
- Updated all scenarios with revised C-SCRM controls.

Appendix C – (NEW) C-SCRM ACTIVITIES IN THE RISK MANAGEMENT PROCESS
- Added discussion of Risk Appetite; expanded discussion of risk tolerance.
- Moved "FARM" from previous Section 2 to this appendix.

Appendix D – (NEW)
- Added C-SCRM templates to include C-SCRM Strategy and Implementation Plan, C-SCRM Policy, C-SCRM Plan, and C-SCRM Risk Assessment.

Appendix E
- Updated to reflect updated SP 800-161 Revision 1 content to include new, changed or deleted glossary terms.

Appendix F
- Updated to reflect updated SP 800-161 Revision 1 content to include new, changed or deleted acronyms.

Appendix G
- Updated references to reflect new, changed or deleted references.

Your feedback on this draft publication is important to us. We appreciate each contribution from our reviewers. The insightful comments from both the public and private sectors, nationally and internationally, continue to help shape the final publication to ensure it meets the needs and expectations of our customers. NIST anticipates producing the second draft of this publication in September 2021 and publishing the final version no later than April 2022. These dates are subject to change.

- JON BOYENS, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: scrm-nist@nist.gov

328 **Table of Contents**

List of Figures

List of Tables

1. INTRODUCTION

Information, communications, and operational technology (ICT/OT) relies on a complex, globally distributed and interconnected supply chain ecosystem that is long, has geographically diverse routes, and consists of multiple levels of outsourcing. This ecosystem is composed of public and private sector entities (e.g., acquirers, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers)[1] and technology, law, policy, procedures, and practices that interact to conduct research and development, design, manufacture, acquire, deliver, integrate operate and maintain, and dispose, and otherwise utilize or manage ICT/OT products and services. This ecosystem has evolved to provide a set of highly refined, cost-effective, reusable solutions. Federal government information systems[2] have rapidly adopted this ecosystem of solution options, which has increased their reliance on commercially available products, system integrator support for custom-built systems, and external service providers. This, in turn, has resulted in increased complexity, diversity, and scale of the federal government's cyber supply chains.

In this document, the term ***supply chain*** refers to the linked set of resources and processes between and among multiple levels of enterprises, each of which is an acquirer that begins with the sourcing of products and services and extends through their life cycle.

Based on this definition, ***cyber supply chain*** is this linked set of resources that can be subject to cyber supply chain risks from suppliers, their supply chains, and their products or services. Cyber supply chain risks include exposures, threats, and vulnerabilities associated with the products and services traversing the supply chain as well as the exposures, threats, and vulnerabilities to the supply chain.

Commercially available technology solutions present significant benefits including low cost, interoperability, rapid innovation, product feature variety, and the ability to choose from competing vendors. These commercial off-the-shelf (COTS) solutions, whether proprietary or open source, can meet the needs of a global base of public and private sector customers. However, the same globalization and other factors that allow for such benefits can also increase the risk of a threat event which can directly or indirectly affect the cyber supply chain—often undetected—and in a manner that may result in risks to the acquirer and the end user.

These cyber supply chain risks may include but are not limited to tainted software, introduction of malware, theft of intellectual property, insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor development and manufacturing practices in the cyber supply chain. These risks are associated with an enterprise's decreased visibility into, and understanding of, how the technology they acquire is developed, integrated, and deployed, as well as the processes, procedures, and practices used to ensure the

[1] See definitions suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers in Appendix F, Glossary.

[2] NIST SP 800-53 Rev. 5 defines Information System as:

An information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial control systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

security, resilience, reliability, safety, integrity, and quality of the products and services.[3] Threats and vulnerabilities created by malicious actors (individuals, enterprises, or nation states) are often especially sophisticated and difficult to detect, and thus provide a significant risk to enterprises. It should be noted that products (including software libraries, frameworks, toolkits, Enterprise Resource Planning (ERP) solutions, and cloud-based resources) or services originating both domestically or abroad might contain vulnerabilities that present opportunities for cyber supply chain compromises.[4] For example, an adversary may have the power to insert malicious capability into a product or to coerce a manufacturer to hand over the manufacturing specifications of a sensitive U.S. system. Note that it is impossible to completely eliminate all cyber supply chain risks.

Currently, enterprises and many private sector suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers use varied and not yet sufficiently standardized practices, which make it difficult to consistently measure and manage cyber supply chain risks across different enterprises.

In this document, the practices and controls described for Cyber Supply Chain Risk Management (C-SCRM) apply to both information technology (IT) and OT environments. Similar to IT environments relying on ICT products and services, OT environments rely on OT and ICT products and services, which create a cyber risk from ICT/OT products, services, suppliers and their supply chains. Organizations should include OT-related suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers within the scope of their C-SCRM activities.

When engaging with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, agencies should carefully consider the breadth of the Federal government's footprint and the high likelihood that individual agencies may enforce varying and conflicting C-SCRM requirements. Overcoming this complexity requires interagency coordination and partnerships. The passage of the Federal Acquisition Supply Chain Security Act (FASCSA) of 2018 aimed to address this concern by creating a government-wide approach to the problem of supply chain security in federal acquisitions by establishing the Federal Acquisition Security Council (FASC). The FASC therefore serves as a focal point of coordination and information sharing and a harmonized approach to acquisition security that addresses C-SCRM in acquisition processes and procurements across the federal enterprise. In addition, the law incorporated SCRM into FISMA by requiring reporting on progress and

[4] This document adapts the definition of risk from [FIPS 200] to establish a definition for cyber supply chain risk as follows:
Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

[4] This document defines a Cyber Supply Chain Compromise as:
Cyber supply chain incident (also known as compromise) is an occurrence within the supply chain whereby the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits is jeopardized. A cyber supply chain incident can occur anywhere during the life cycle of the system, product or service.

[5] Appendix F, Glossary

effectiveness of the agency's supply chain risk management consistent with guidance issued by the Office of Management and Budget and the Council.

1.1. PURPOSE

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 cyber supply chain risks presented by the supplier, the supplied products and services, or the supply chain.[5] The purpose of this publication is to provide guidance to organizations on how to identify, assess, select, and implement risk management processes and mitigating controls across the organization to help manage cyber supply chain risks.

The processes and controls identified in this document can be modified or augmented with organization-specific requirements from policies, guidelines, response strategies, and other sources. This publication empowers organizations to develop C-SCRM strategies that are tailored to their specific mission/business needs, threats, and operational environments.

1.2. TARGET AUDIENCE

C-SCRM is an organization-wide activity that should be directed under the overall enterprise governance, regardless of the specific organizational structure.

This publication is intended to serve a diverse audience involved in C-SCRM, including:

- Individuals with system, information security, privacy, or risk management and oversight responsibilities, including authorizing officials (AOs), chief information officers, senior information security officers, and senior officials for privacy;
- Individuals with system development responsibilities, including mission or business owners, program managers, system engineers, system security engineers, privacy engineers, hardware and software developers, system integrators, and acquisition or procurement officials;
- Individuals with acquisition and procurement-related responsibilities, including acquisition officials and contracting officers;
- Individuals with logistical or disposition-related responsibilities, including program managers, procurement officials, system integrators, and property managers;
- Individuals with security and privacy implementation and operations responsibilities, including mission or business owners, system owners, information owners or stewards, system administrators, continuity planners, and system security or privacy officers;
- Individuals with security and privacy assessment and monitoring responsibilities, including auditors, Inspectors General, system evaluators, control assessors, independent verifiers and validators, and analysts; and

592 • Commercial entities, including industry partners, that produce component products and
593 systems, create security and privacy technologies, or provide services or capabilities that
594 support information security or privacy.

595 **1.3. BACKGROUND**
596
597 C-SCRM encompasses activities that span the entire system development life cycle (SDLC),
598 including research and development, design, manufacturing, acquisition, delivery, integration,
599 operations and maintenance, disposal, and overall management of an organization's products and
600 services. C-SCRM lies at the intersection of security, resilience, reliability, safety, integrity, and
601 quality, as depicted in Figure 1-1.
602

603
604 **Fig. 1-1: Dimensions of C-SCRM**

605 • Security provides the confidentiality, integrity, and availability of information that (a)
606 describes the cyber supply chain (e.g., information about the paths of products and
607 services, both logical and physical) or (b) traverses the cyber supply chain (e.g.,
608 intellectual property contained in products and services), as well as information about the
609 parties participating in the cyber supply chain (anyone who touches a product or service
610 throughout its life cycle);
611 • Resilience is focused on ensuring the cyber supply chain will provide required products
612 and services and these products and services will be able to sufficiently perform or
613 recover, under stress or failure;

- Reliability is focused on the ability of a product or service to function as defined for a specified period of time in a predictable manner;[6]
- Safety is focused on ensuring the product or service are free from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment;[7]
- Integrity is focused on ensuring the products or services in the cyber supply chain are genuine, unaltered, and the products and services will perform according to acquirer specifications and without additional unwanted functionality; and
- Quality is focused on meeting or exceeding performance, technical, and functional specifications while ensuring vulnerabilities are mitigated that may limit the intended function of a component or delivery of a service, lead to component or service failure, or provide opportunities for exploitation.

1.3.1. The Business Case for C-SCRM

Today, every organization heavily relies on digital technology to fulfill its business and mission. Digital technology is comprised of ICT/OT products and is delivered through and supported by services. C-SCRM is a critical capability that every organization needs to have to address cyber risks posed by the use of digital technology to support its business and mission. The depth, extent, and maturity of a C-SCRM capability for each organization should be based on the uniqueness of business or mission, organization-specific compliance requirements, operational environment, risk appetite, and risk tolerance.

Establishing and sustaining a C-SCRM capability creates a number of significant benefits:

- Reduced likelihood of cyber supply chain compromise. Well-designed C-SCRM processes and controls achieve this by enhancing an organization's ability to effectively detect, respond, and recover from events that result in significant business disruptions, should a C-SCRM compromise occur.
- Operational and organizational efficiencies achieved through clear structure, purpose, and alignment of C-SCRM capabilities and prioritization, consolidation, and streamlining of existing C-SCRM processes.
- Greater assurance that products acquired are of high quality, authentic, reliable, resilient, maintainable, secure, and safe.

Greater assurance that service providers are trustworthy and can be relied upon to meet their performance requirements. Organizations should carefully consider the potential costs of applying C-SCRM processes and controls, weighing such costs against the risk to the organization were they not applied. Implementing C-SCRM processes and controls will require financial and human resources, as well as tools and infrastructure investments, not only from the organizations themselves, but also from their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers which may also result in increased costs to the acquirer. Such costs may be realized through required staff upskilling or

[6] NIST SP 800-160 Vol.2
[7] NIST SP 800-160 Vol.2

hiring, vendor switching, impacts on contingency planning, supplier diversity, and procurement timeline delays.

The passage of the 2018 SECURE Technology Act, formation of the Federal Acquisition Security Council (FASC), and the observations from the 2015 and 2019 Case Studies in Cyber Supply Chain Risk Management captured in the National Institute of Standards and Technology Interagency Report (NISTIR) 8276, *Key Practices in Cyber Supply Chain Risk Management*, point to broad public and private sector consensus: C-SCRM capabilities are a critical and foundational component of any organization's risk posture.

1.3.2. Organization's Cyber Supply Chain

Today's organizations run complex information systems and networks to support their missions. These information systems and networks are composed of ICT/OT[8] products and components made available by *suppliers, developers, and system integrators*. Organizations also acquire and deploy an array of services, that include but are not limited to:

- Building custom software for information systems that are to be deployed within the organization, made available by *developers;*
- Integrating or providing operations, maintenance, and disposal support for information systems and networks within and outside of the organization's boundaries,[9] made available by *system integrators or other ICT/OT-related service providers;* and
- Providing external services to support organization's operations that are positioned both inside or outside of the authorization boundaries, made available by *external system service providers*.

These services may span the entire SDLC for an information system or service and may be:

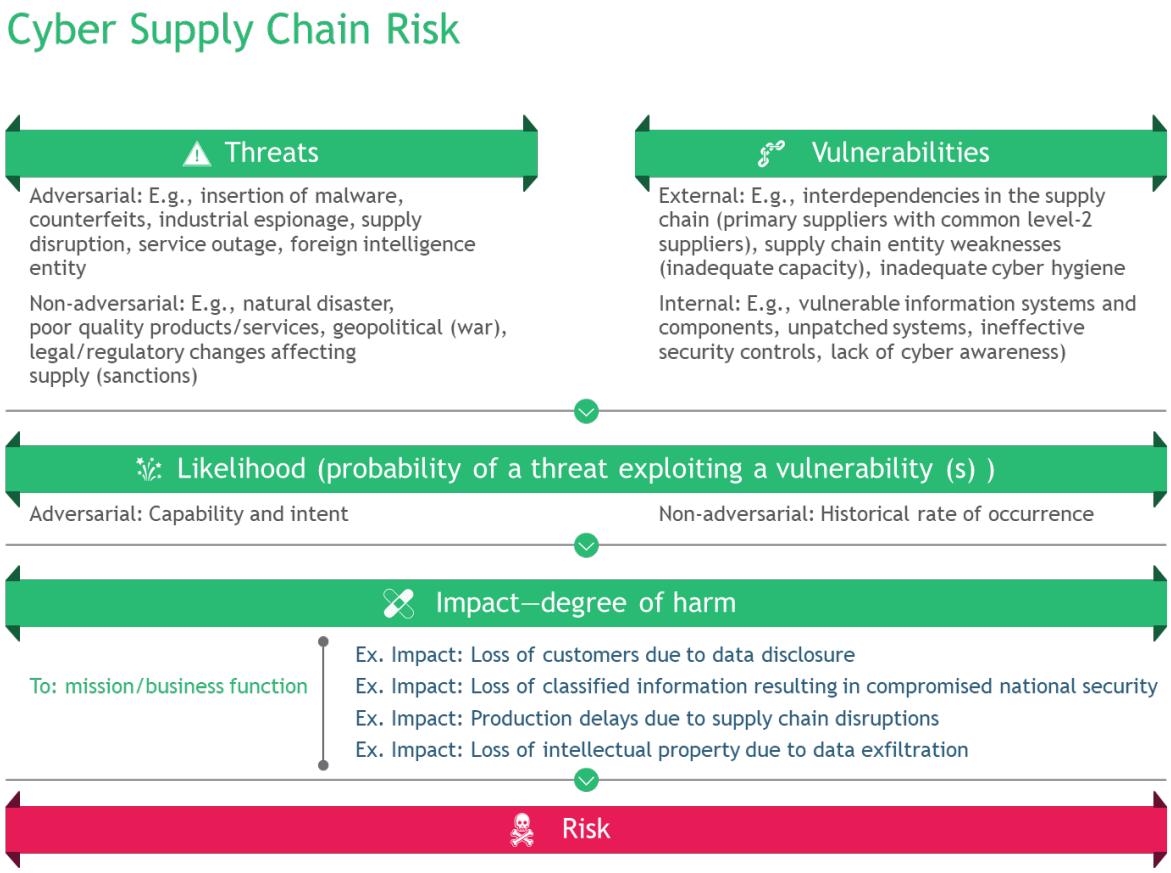
- Performed by the staff employed by the organization, developer, system integrator, or external system service provider;
- Be physically hosted by the organization or by the developer, system integrator, or external system service provider;
- Supported or comprised of development environments, logistics/delivery environments that transport information systems and components, or applicable system and communications interfaces;
- Using Commercial-off-the-Shelf (COTS) hardware and software.

[8] NIST SP 800-37 Rev. 2 defines Operational Technology as:
Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

[9] For federal information systems, this is the Authorization Boundary, defined in NIST SP 800-53 Rev. 5 as:
All components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected.

694 The responsibility and accountability for the services and associated activities performed by
695 different parties within this ecosystem are usually defined by agreement documents between the
696 organization and suppliers, developers, system integrators, external system service providers, and
697 other ICT/OT-related service providers.
698

699 ### 1.3.3. Cyber Supply Chain Risk
700
701 Cyber supply chain risks include, but are not limited to, the insertion of counterfeits,
702 unauthorized production, malicious insiders, tampering, theft, insertion of malicious software
703 and hardware (e.g., Global Positioning System (GPS) tracking devices, computer chips, etc.), as
704 well as poor manufacturing and development practices in the cyber supply chain. These risks are
705 realized when threats in the cyber supply chain exploit existing vulnerabilities.
706
707 Figure 1-2 depicts cyber supply chain risk resulting from the likelihood that relevant threats may
708 exploit applicable vulnerabilities and the consequential potential impact.
709



710

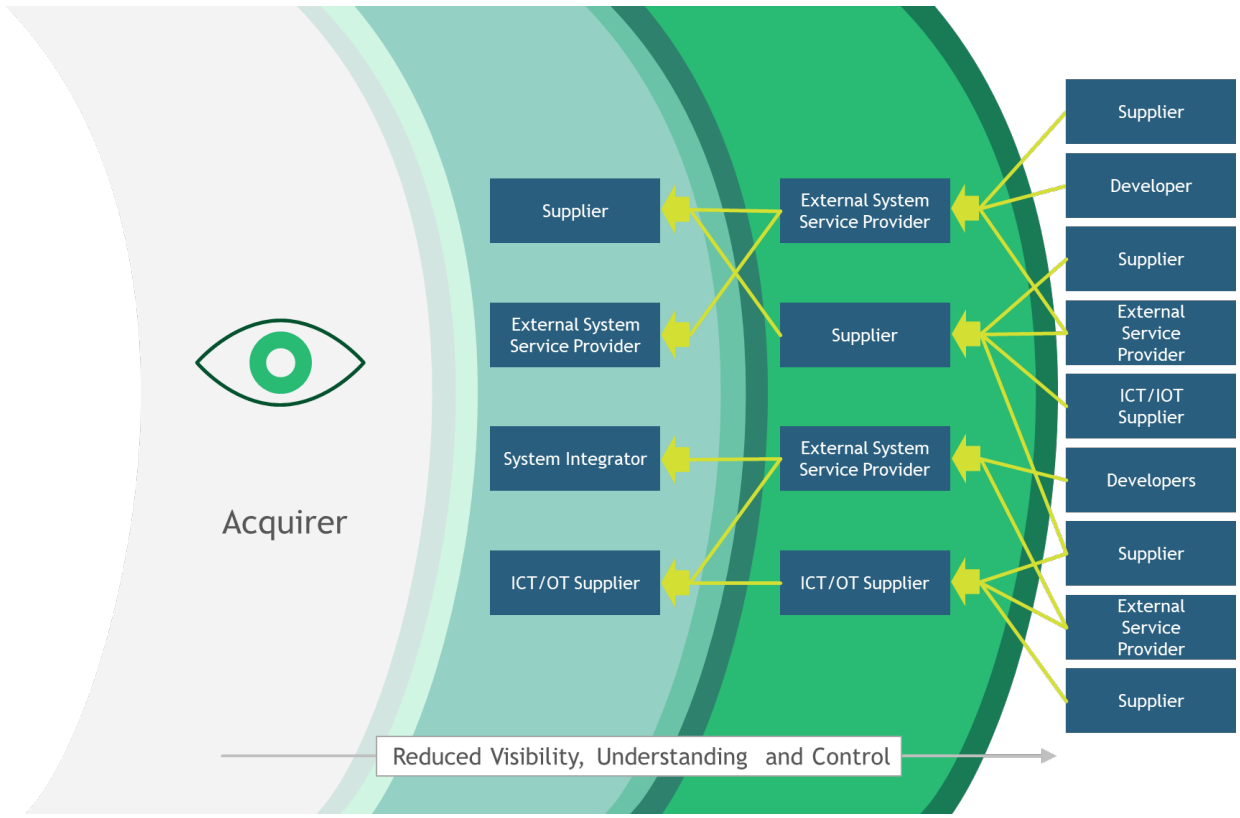
711 **Fig. 1-2: Cyber Supply Chain Risk**

712 Cyber supply chain vulnerabilities may lead to a persistent negative impact on an organization's
713 missions ranging from reduction in service levels leading to customer dissatisfaction to theft of

714 intellectual property or degradation of critical mission and business processes. However, it
715 might take years for such vulnerability to be exploited or discovered. It may also be difficult to
716 determine whether an event was the direct result of a supply chain vulnerability. Shared
717 vulnerabilities in the supply chain may also expose organizations to cascading cyber supply
718 chain risks. For example: a large-scale service outage at a major cloud services provider may
719 cause service or production disruptions for multiple entities within an organization's supply
720 chain and lead to negative effects within multiple mission and business processes.
721

722 ### 1.3.4. Supplier Relationships within Organizations
723
724 Cyber supply chain risks are associated with an organization's decreased visibility into, and
725 understanding of, how the technology they acquire is developed, integrated, and deployed and
726 how the services they acquire are delivered. They are also associated with the processes,
727 procedures, and practices used to ensure the security, safety, integrity, quality, reliability,
728 trustworthiness or authenticity of a product, service or source of the products and services.
729 Federal agencies have a variety of relationships with their suppliers, developers, system
730 integrators, external system service providers, and other ICT/OT-related service providers.
731 Figure 1-3 depicts how these diverse types of relationships affect an organization's visibility and
732 control of the supply chain.
733
734

735



736

737 **Fig. 1-3: An Organization's Visibility, Understanding, and Control of its Cyber Supply**
738 **Chain**

739 Some supply chain relationships are tightly intermingled, such as the development by a system
740 integrator of a complex information system designed to operate within the federal agency's
741 authorization boundary, or the management of federal agency information systems and resources
742 by an external service provider. These relationships are usually guided by an agreement (e.g.,
743 contract) that establishes detailed functional, technical, and security requirements and may
744 provide for custom development or significant customization of products and services. For these
745 relationships, system integrators and external service providers are likely able to work with the
746 organization to implement such processes and controls (listed within this document) which are
747 deemed appropriate based on the results of a criticality and risk assessment and cost/benefit
748 analysis. This may include floating requirements upstream in the supply chain to ensure higher
749 confidence in the satisfaction of necessary assurance objectives. The decision to extend such
750 requirements must be balanced with an appreciation of what is feasible and cost-effective. The
751 degree to which system integrators and external service providers are expected to implement C-
752 SCRM processes and controls should be weighed against the risks to the organization posed by
753 not adhering to those additional requirements. Often, working directly with the system
754 integrators and external service providers to proactively identify appropriate mitigation processes
755 and controls will help create a more cost-effective strategy.
756

Procuring ICT/OT products directly from suppliers establishes a direct relationship between those suppliers and the acquirers. This relationship is also usually guided by an agreement between the acquirer and the supplier. However, commercial ICT/OT developed by suppliers are typically designed for general purposes for a global market and are not typically tailored to an individual customer's specific operational or threat environments. Organizations should perform due diligence research regarding their specific C-SCRM requirements to determine if an IT solution is "fit for purpose[10]," includes requisite security features and capabilities, will meet quality and resiliency expectations, and if and how the supplier will provide support for the product, or product components, over its life cycle.

An assessment of the findings of an acquirer's research about a product—which may include engaging in a dialog directly with suppliers whenever possible—will help acquirers understand the characteristics and capabilities of existing ICT/OT products and services, set expectations and requirements for suppliers, and identify C-SCRM needs not yet satisfied by the market. It can also help identify emerging solutions that may at least partially support the acquirer's needs. Overall, such research and engagement with a supplier will allow the acquirer to better articulate their requirements to align with and drive market offerings and make risk-based decisions about product purchases, configurations, and usages within their environment.

Managing Cost and Resources

Balancing cyber supply chain risks with the costs and benefits of C-SCRM controls should be a key component of the acquirer's overall approach to C-SCRM.

Organizations should be aware that implementing C-SCRM controls necessitates additional financial and human resources. Requiring a greater level of testing, documentation, or security features from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers may increase the price of a product or service which may result in increased cost to the acquirer. This is especially true for those products and services developed for general-purpose application and not tailored to the specific organization's security or C-SCRM requirements. In the decision whether to require and implement C-SCRM controls, acquirers should consider both the costs of implementing these controls and the risks of not implementing them.

To mitigate the costs and when appropriate, acquirers should allow suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers the opportunity to reuse any existing data and documentation that may provide evidence to support C-SCRM.

[10] "Fit for purpose" is a term used informally to describe a process, configuration item, IT service, etc., that is capable of meeting its objectives or service levels. Being fit for purpose requires suitable design, implementation, control, and maintenance. (Adapted from Information Technology Infrastructure Library (ITIL) Service Strategy [ITIL Service Strategy].)

1.4. C-SCRM KEY PRACTICES

Cyber supply chain risk management builds on existing standardized practices in multiple disciplines, as well as the evolution of C-SCRM capabilities. Organizations should prioritize reaching a base level of maturity in key practices prior to specifically focusing on advanced C-SCRM capabilities. Those key practices are described in NIST standards and guidelines, such as NISTIR 8276, as well as other applicable national and international standards and best practices. They include: integrating C-SCRM across the organization; establishing a formal program; knowing and managing critical products, services, and suppliers; understanding an organization's supply chain; closely collaborating with key suppliers; including key suppliers in resilience and improvement activities; assessing and monitoring throughout the supplier relationship; and, planning for the full lifecycle.

1.4.1. Foundational Practices

Having foundational practices in place is critical to successfully and productively interacting with system integrators and suppliers may be at varying levels themselves regarding having such practices standardized and in place. The following are specific examples of the recommended multidisciplinary foundational practices that can be implemented incrementally to improve an organization's ability to develop and execute more advanced C-SCRM practices:

- Establish a core, dedicated multi-disciplinary C-SCRM Program Management Office and/or C-SCRM team;
- Implement a risk management hierarchy and risk management process (in accordance with NIST SP 800-39, *Managing Information Security Risk* [NIST SP 800-39]) including an organization-wide risk assessment process (in accordance with NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [NIST SP 800-30 Rev. 1]);
- Establish an organization governance structure that integrates C-SCRM requirements and incorporates these requirements into the organizational policies;
- Develop a process for identifying and measuring the criticality of the organization's suppliers, products and services;
- Raise awareness and foster understanding of what C-SCRM is and why it is critically important;
- Develop and/or integrate C-SCRM into acquisition/procurement policies and procedures (including Federal Information Technology Acquisition Reform Act (FITARA) processes, applicable to federal agencies) and purchase card processes;
- Establish consistent, well-documented, repeatable processes for determining [Federal Information Processing Standards (FIPS) 199] impact levels;
- Establish and begin using supplier risk assessment processes on a prioritized basis (inclusive of criticality analysis, threat analysis, and vulnerability analysis) after the [FIPS 199] impact level has been defined;
- Implement a quality and reliability program that includes quality assurance and quality control process and practices;
- Establish explicit collaborative and discipline-specific roles, accountabilities, structures, and processes for supply chain, cybersecurity, product security, and physical security

(and other relevant) processes (e.g., Legal, Risk Executive, Human Resources (HR), Finance, Enterprise IT, Program Management/System Engineering, Information Security, Acquisition/procurement, supply chain logistics, etc.);

- Ensure that adequate resources are dedicated and allocated to information security and C-SCRM to ensure proper implementation of policy, guidance, and controls;
- Ensure there are sufficiently cleared personnel, with key C-SCRM roles and responsibilities, to access and share C-SCRM-related classified information.
- Implement an appropriate and tailored set of baseline information security controls found in NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations [NIST SP 800-53 Rev. 5];
- Establish internal checks and balances to ensure compliance with security and quality requirements;
- Establish a supplier management program including, for example, guidelines for purchasing directly from qualified original equipment manufacturers (OEMs)[11] or their authorized distributors and resellers; and
- Implement a robust incident management program to successfully identify, respond to, and mitigate security incidents. This program should be capable of identifying causes of security incidents, including those originating from the cyber supply chain.

1.4.2. Sustaining Practices

Sustaining practices should be used to enhance the efficacy of cyber supply chain risk management. These practices are inclusive of and build upon foundational practices. Organizations that have standardized and implemented the foundational practices broadly should consider these practices as next steps in advancing their cyber supply chain risk management capabilities:

- Use third-party assessments, site visits, and formal certification to assess critical suppliers;
- Use the organization's understanding of its C-SCRM risk profile (or risk profiles, specific to mission/business areas) to define a risk appetite and risk tolerances to empower leaders with delegated authority across the organization to make C-SCRM decisions in alignment with organization's mission imperatives and its strategic goals and objectives;
- Use a formalized information sharing function to engage with the FASC as well as other government agencies to enhance the organization's cyber supply chain threat and risk insights and help ensure a coordinated and holistic government-wide approach to addressing cyber-supply chain risks that may affect a broader set of agencies or national security;
- Embed C-SCRM specific training into training curriculums of applicable roles across the organization processes involved with C-SCRM including but not limited to information security, procurement, risk management, engineering, software development, IT, legal, and HR;

[11] For purposes of this publication, the term *original equipment manufacturers* includes *original component manufacturers*.

- Integrate C-SCRM considerations into every aspect of the system and product lifecycle, implementing consistent, well-documented, repeatable processes for system engineering, cybersecurity practices, and acquisition;
- Integrate the organization's defined C-SCRM requirements into contractual language found in agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers;
- Include key suppliers in contingency planning, incident response, and disaster recovery planning and testing;
- Engage with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to improve their cybersecurity practices; and
- Define, collect and report C-SCRM metrics to ensure cyber supply chain risk aware leadership, enable active management of the completeness of C-SCRM implementations, and drive efficacy of the organization's C-SCRM processes and practices.

1.4.3. Enhancing Practices

Enhancing practices should be applied by the organization with the goal of advancement toward adaptive and predictive C-SCRM capabilities. Organizations should pursue these practices once sustaining practices have been broadly implemented and standardized across the organization:

- Automate C-SCRM processes where applicable and practical to drive execution consistency, efficiency, and free up key resources to focus on other critical C-SCRM activities;
- Adopt quantitative risk analyses that apply probabilistic approaches (e.g. Bayesian Analysis, Monte Carlo Methods) to reduce uncertainty about cyber supply chain risk, enhance organization leadership's ability to identify optimal risk responses, and measure response effectiveness; and
- Apply insights gained from leading C-SCRM metrics (i.e., forward-looking indicators) to shift from reactive to predictive C-SCRM strategies and plans that adapt to cyber supply chain risk profile changes before they occur.

The guidance and controls contained in this publication are built on existing multidisciplinary practices and are intended to increase the ability of organizations to strategically manage cyber supply chain risks over the entire life cycle of systems, products, and services. Refer to Table 3-3 in Section 3 for a summary view of C-SCRM key practices.

1.5. RELATIONSHIP TO OTHER PROGRAMS AND PUBLICATIONS

The revision to NIST SP 800-161 builds upon concepts described in a number of NIST and other publications to facilitate integration with the agencies' existing organization-wide activities, as well as a series of legislative developments following its initial release. These resources are complementary and help organizations build risk-based information security programs to protect their operations and assets against a range of diverse and increasingly sophisticated threats. This publication will be revised to remain consistent with the NIST SP 800-53 security controls catalog, using an iterative process as the C-SCRM discipline continues to mature.

1.5.1. NIST Publications

NIST SP 800-161 Rev. 1 leverages the latest versions of the publications and programs that guided its initial development, as well as new publications following its initial release:

- NIST Cybersecurity Framework (CSF) Version 1.1;
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems,* to conduct criticality analysis to scoping C-SCRM activities to high-impact components or systems [FIPS 199];
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments,* to integrate ICT/OT SCRM into the risk assessment process [NIST SP 800-30 Rev. 1];
- 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 800-37 Rev. 2]*;*
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View,* to integrate ICT/OT SCRM into the risk management levels and risk management process [NIST SP 800-39];
- NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* to provide information security controls for enhancing and tailoring to C-SCRM context [NIST SP 800-53 Rev. 5];
- NIST SP 800-53B Revision 5, *Control Baselines for Information Systems and Organizations*, to codify control baselines and C-SCRM supplementary guidance and [NIST SP 800-53B Rev. 5];
- NIST SP 800-160 Vol. 1, *Systems Security Engineering* [NIST SP 800-160 Vol. 1] and NIST SP 800-160 Vol. 2, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach* [NIST SP 800-160 Vol. 2] for specific guidance on the security engineering aspects of C-SCRM;
- NIST SP 800-181 Revision 1, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, as a means of forming a common lexicon on C-SCRM workforce topics [NIST SP-800-181 Rev. 1];
- NISTIR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*, for background materials in support of applying the special publication to their specific acquisition processes [NISTIR 7622];
- NISTIR 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components*, to guide ratings of supplier criticality [NISTIR 8179];
- NISTIR 8272, *Impact Analysis Tool for Interdependent Cyber Supply Chain Risks* for guidance on how to prioritize supplier criticality [NISTIR 8272];
- NISTIR 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*, to elucidate recent C-SCRM trends in the private sector [NISTIR 8276]; and
- NISTIR 8286, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)*, to inform the content on integrating C-SCRM into enterprise risk management [NISTIR 8286].

1.5.2. Regulatory and Legislative Guidance

NIST SP 800-161 Rev. 1 is informed heavily by the regulatory and legislative guidance, including:

- Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*; and
- The Federal Acquisition Supply Chain Security Act (FASCA), *Title II of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology Act of 2018*.

1.5.3. Other U.S. Government Reports

NIST SP 800-161 Rev. 1 is also informed by a number of additional government reports:

- Government Accountability Office (GAO) Report, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, December 2020, GAO-21-171 [GAO]
- Department of Defense and Department of Homeland Security Software Assurance Acquisition Working Group, *Software Assurance in Acquisition: Mitigating Risks to the Enterprise* [SwA];
- National Defense Industrial Association (NDIA), *Engineering for System Assurance* [NDIA];

1.5.4. Standards, Guidelines, and Best Practices

Additionally, NIST SP 800-161 draws its inspiration from a number of international standards, guidelines, and best practice documents:

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15288 – *Systems and software engineering – System Life Cycle Processes* [ISO/IEC 15288];
- ISO/IEC 27036 – *Information Technology – Security Techniques – Information Security for Supplier Relationships* [ISO/IEC 27036];
- ISO/IEC 20243 – *Information Technology — Open Trusted Technology Provider™ Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products* [ISO/IEC 20243];
- ISO/IEC 27000 – *Information Technology – Security Techniques – Information Security Management System – Overview and Vocabulary* [ISO/IEC 27000];
- ISO/IEC 27002 – *Information Technology – Security Techniques – Code of Practice for Information Security Controls* [ISO/IEC 27002];
- Software Assurance Forum for Excellence in Code (SAFECode) *Software Integrity Framework* [SAFECode 2] and *Software Integrity Best Practices* [SAFECode 1]; and
- Cyber Risk Institute, *Financial Services Cybersecurity Framework Profile Version 1.1* [FSP].

1.5.5. Guidance for Cloud Service Providers

The *external system service providers* discussed in this publication include *cloud service providers*. This publication does not replace guidance provided with respect to federal agency

assessment of cloud service providers' security. When applying this publication to cloud service providers, federal agencies should first use Federal Risk and Authorization Program (FedRAMP) cloud services security guidelines and then apply NIST SP 800-161 Rev. 1 for those processes and controls that are not addressed by FedRAMP. [12]

1.6. METHODOLOGY FOR BUILDING C-SCRM GUIDANCE USING SP 800-39, SP 800-37 REVISION 2, AND NIST SP 800-53 REVISION 5

This publication applies the multileveled risk management approach of [NIST SP 800-39], by providing C-SCRM guidance at organization, mission, and operational-levels. It also introduces a navigational system for SP 800-37 Rev. 2, allowing users to more easily focus on relevant sections of this publication. Finally, it contains an enhanced overlay of specific C-SCRM controls, building on NIST SP 800-53 Revision 5.

The guidance/controls contained in this publication are built on existing multidisciplinary practices and are intended to increase the ability of organizations to strategically and operationally manage the associated cyber supply chain risks over the entire life cycle of systems, products, and services. It should be noted that this publication gives organizations the flexibility to either develop stand-alone documentation (e.g., policies, assessment and authorization [A&A] plan and C-SCRM plan) for C-SCRM or to integrate it into existing agency documentation.

For individual systems, this guidance is recommended for use with information systems at all impact categories, according to [FIPS 199]. The agencies may choose to prioritize applying this guidance to systems at a higher-impact level or to specific system components. Finally, NIST SP 800-161 Rev. 1 describes the development and implementation of C-SCRM Strategies and Implementation Plans for development at the enterprise and mission/business level of an organization and a C-SCRM system plan at the operational level of an organization. A C-SCRM plan at the operational level is informed by the cyber supply chain risk assessment and should contain C-SCRM controls tailored to specific agency mission/business needs, operational environments, and/or implementing technologies.

1.6.1. Integration into Risk Management Process

The processes in this publication should be integrated into agencies' existing SDLCs and organizational environments at all levels of risk management processes and hierarchy (organization, mission, system) as described in [NIST SP 800-39]. Section 2 provides an overview of the [NIST SP 800-39] risk management hierarchy and approach and identifies C-SCRM activities in the risk management process. Appendix C builds on Section 2 of [NIST SP 800-39], providing descriptions and explanations of ICT/OT SCRM activities. The structure of Appendix C mirrors [NIST SP 800-39].

[12] For cloud services, FedRAMP is applicable for low-, moderate-, high-impact systems [FedRAMP]. Ongoing work will address high-impact systems utilizing cloud services. Once the work is completed, agencies should refer to FedRAMP for guidance applicable to high-impact systems utilizing cloud services.

1.6.2. Implementing C-SCRM in the Context of SP 800-37 Revision 2

C-SCRM activities described in this publication are closely related to the Risk Management Framework described in [NIST SP 800-37, Rev. 2]. Specifically, C-SCRM processes conducted at the operational level should closely mirror and/or serve as inputs to those steps completed as part of the [NIST SP 800-37, Rev 2]. C-SCRM activities completed at Levels 1 and 2 should provide inputs (e.g., risk assessment results) to the operational-level, RMF-type processes where possible and applicable. Section 2 and Appendix C describe in further detail the linkages between C-SCRM and [NIST SP 800-37, Rev. 2].

1.6.3. Enhanced C-SCRM Overlay

This publication contains an enhanced overlay of [NIST SP 800-53 Rev. 5]. Appendix A identifies, refines, and expands C-SCRM-related controls from [NIST SP 800-53 Rev. 5], adds new controls that address specific C-SCRM concerns, and offers C-SCRM-specific supplemental guidance where appropriate. Figure 1-4 illustrates the process used to create the enhanced overlay. The individual controls and enhancements from [NIST SP 800-53 Rev. 5] that were relevant to C-SCRM were extracted. These controls were analyzed to determine how they apply to C-SCRM. Additional supplemental guidance was then developed and included for each control and control enhancement. The resulting set of controls and enhancements were evaluated to determine whether all C-SCRM concerns were addressed.

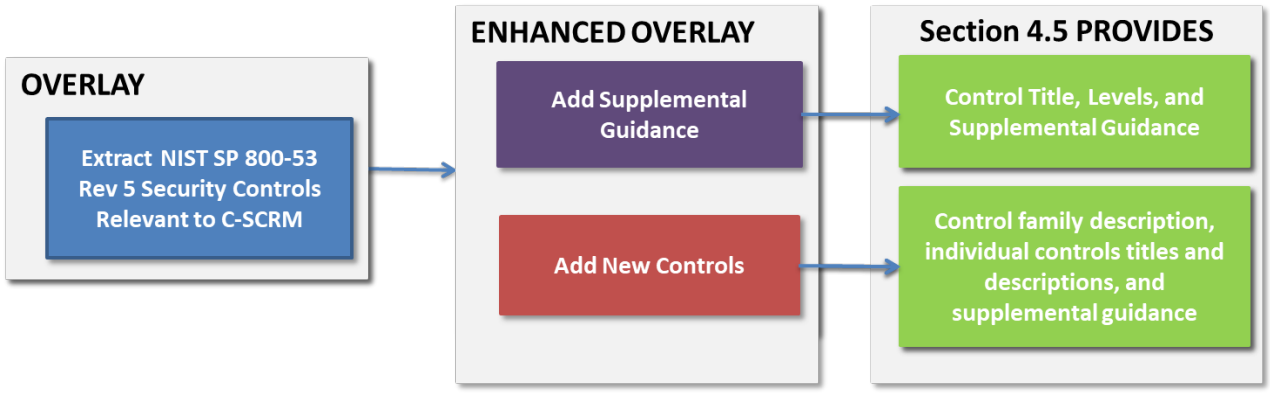


Fig. 1-4: C-SCRM Security Controls in NIST SP 800-161, Revision 1, Section 4.5

1.7. ORGANIZATION OF THIS SPECIAL PUBLICATION

This publication is organized as follows:

- Section 1 provides the purpose, scope, and applicability of the publication and describes foundational concepts and practices;
- Section 2 discusses C-SCRM processes and how to integrate them into the organizational risk management hierarchy and risk management process, based on NIST SP 800-39;
- Section 3 discusses critical success factors for C-SCRM;

- Section 4 contains implementation guidance for C-SCRM controls;
- Appendix A provides C-SCRM controls summary;
- Appendix B provides a set of example cyber supply chain risk exposure scenarios;
- Appendix C provides C-SCRM activities in the Risk Management Process;
- Appendix D provides a set of C-SCRM templates to include C-SCRM Strategy and Implementation Plan, C-SCRM Policy, C-SCRM Plan and C-SCRM Risk Assessment;
- Appendix E provides a glossary of terms used in the publication;
- Appendix F provides the acronyms and abbreviations used in the publication;
- Appendix G lists references used in the development of this publication.

2. INTEGRATION OF C-SCRM INTO ENTERPRISE-WIDE RISK MANAGEMENT

C-SCRM should be integrated into the enterprise-wide risk management process described in [NIST SP 800-39] and depicted in Figure 2-1. This process includes the following continuous and iterative steps:

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

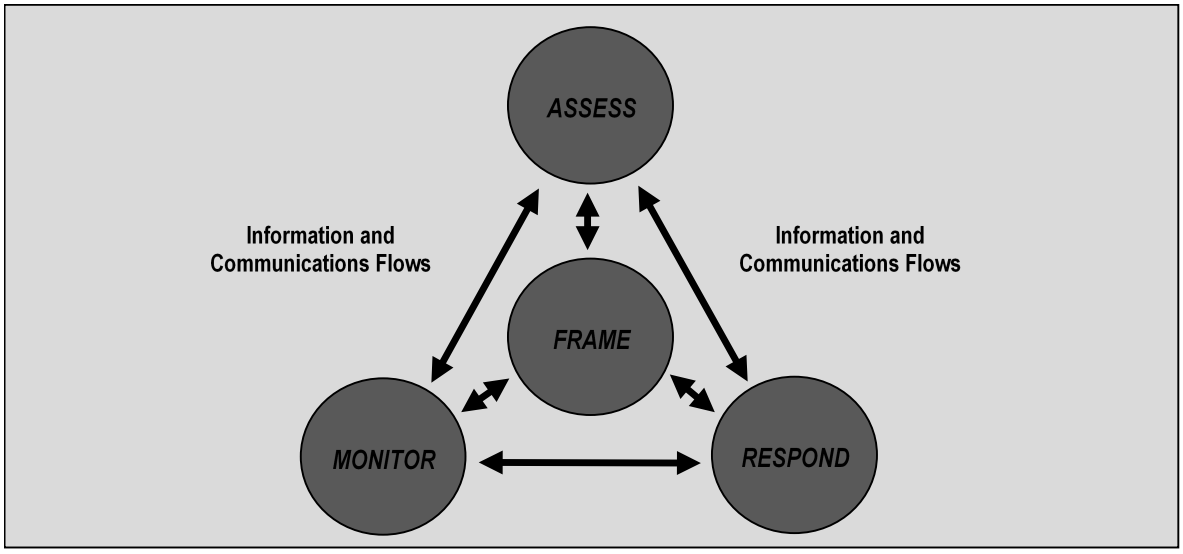


Fig. 2-1: Risk Management Process

Managing cyber supply chain risks is a complex undertaking that requires a coordinated, interdisciplinary approach across an organization. Effective cyber supply chain risk management (C-SCRM) requires engagement from stakeholders inside the organization (e.g., departments, processes) as well as outside the organization (e.g., suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers) to actively collaborate, communicate, and take actions to secure favorable C-SCRM outcomes. Organizations should aim to infuse perspectives from multiple disciplines and processes (e.g., information security, procurement, enterprise risk management, engineering, software development, IT, legal, HR, etc.) into their approaches to managing cyber supply chain risk. Organizations may define explicit roles to bridge and integrate these processes as a part of an organization's broader risk management activities. This orchestrated approach is an integral part of an organization's effort to identify C-SCRM priorities, develop solutions, and incorporate C-

SCRM into overall risk management decisions. Organizations should perform C-SCRM activities as a part of acquisition, SDLC, and broader organizational risk management processes. Embedded C-SCRM activities involve identifying and assessing applicable risks, determining appropriate mitigating actions, documenting selected risk response actions, and monitoring performance of C-SCRM activities. As exposure to supply chain risk differs across organizations, enterprise and mission-specific strategies and policies should set the tone and direction for C-SCRM across the organization.

Organizations should ensure that tailored C-SCRM plans are designed to:

- Manage, rather than eliminate risk;
- Ensure that operations are able to adapt to constantly emerging or evolving threats;
- Be responsive to changes within their own organization, programs, and the supporting information systems; and
- Adjust to the rapidly evolving practices of the private sector's global ICT supply chain.

Section 2.1 describes the three-level risk management approach in terms of C-SCRM. Generally, senior leaders provide the strategic direction, mid-level leaders plan and manage programs and projects, and individuals on the front lines procure, develop, implement, and operate the products and perform the services in their supply chain. As part of a multifaceted approach, organizations may rely on a centralized, interdisciplinary team or program management office (PMO) to lead, perform, and coordinate Level 1 and Level 2 C-SCRM processes that inform C-SCRM processes at the Level 3 operational-level. Specific discussion of the full scope of C-SCRM PMO implementations and responsibilities is discussed later in this section. In general, the activities performed in each level can be integrated into an organization's overall risk management process in order to ensure that the C-SCRM program appropriately supports the organization's mission and goals.[13] Section 2.2 describes the Risk Management Framework as it applies to C-SCRM. The foundational concepts are described in greater detail in [NIST SP 800-39].

[13] This document uses the word "mission" to mean the organization's required tasks as determined by the organization's purpose and enterprise-level goals and priorities.

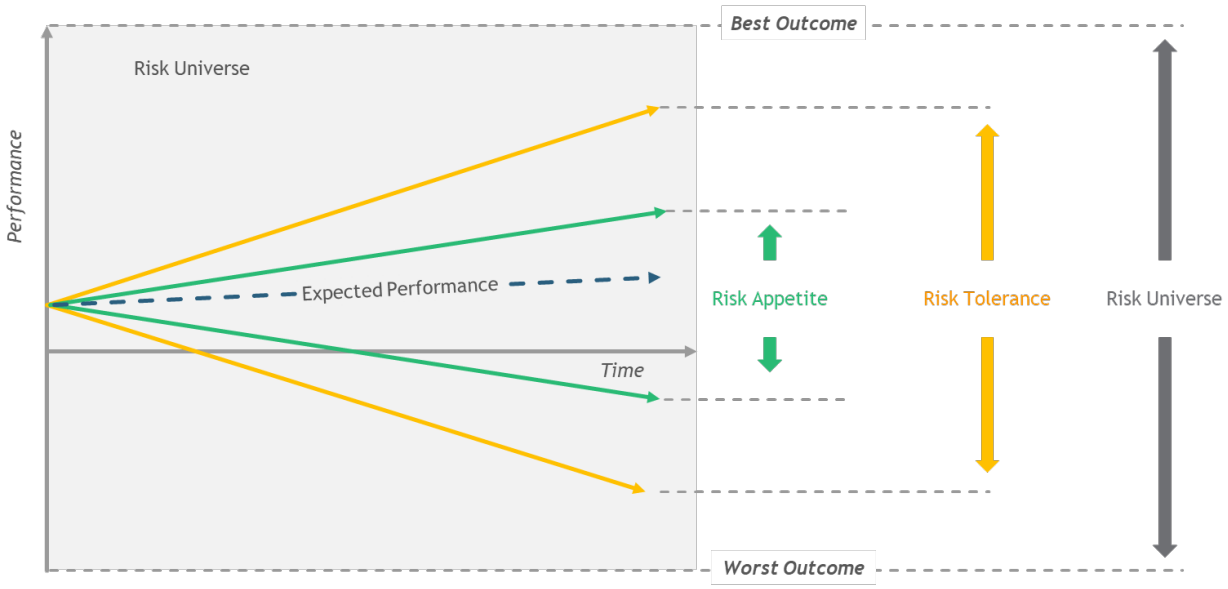


Fig. 2-2: Risk Appetite & Risk Tolerance

Risk Appetite and Risk Tolerance play a critical role in enabling organizations to effectively manage exposure to cyber supply chain risks:

- Risk appetite represents the types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value [NISTIR 8286];
- Risk tolerance is the acceptable level of variation relative to achievement of a specific value objective;
- Risk appetite provides the management's expected bounds for taking risks in pursuit of value while risk tolerance provides the bounds not be exceeded;
- Refer to the appendix for further discussion on Risk Appetite & Risk Tolerance.

2.1. Multi-Level Risk Management

To integrate risk management throughout an organization, [NIST SP 800-39] describes three levels, depicted in Figure 2-2, that address risk from different perspectives: (i) enterprise-level; (ii) mission/business process level; and (iii) operational level. C-SCRM requires the involvement of all three levels.

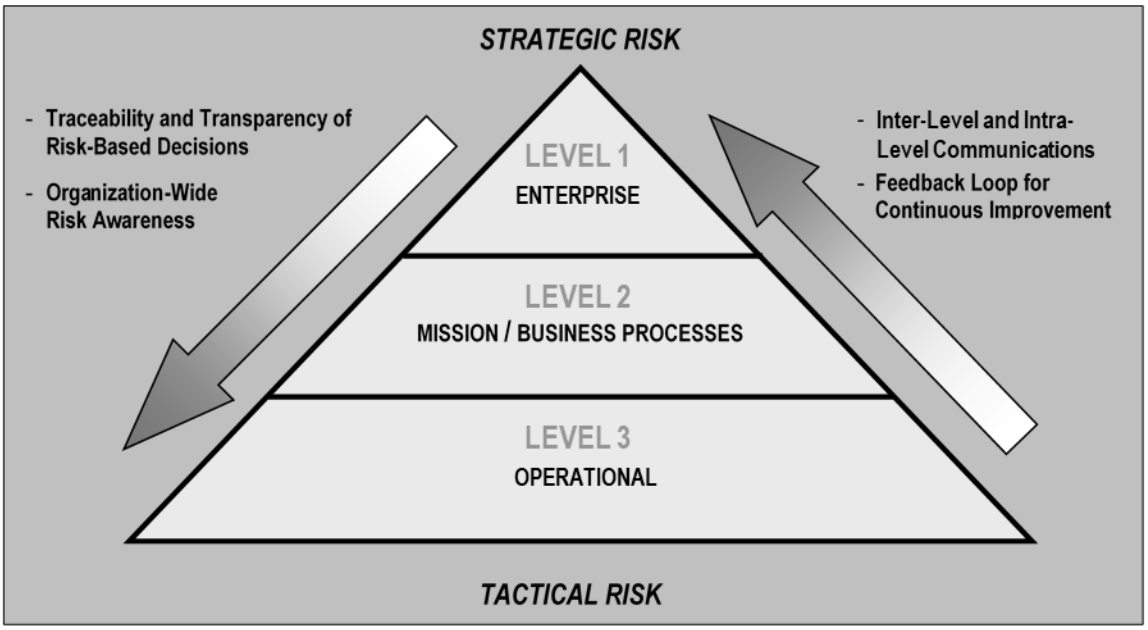


Fig. 2-3: Multileveled Organization-wide Risk Management[14]

In general, Level 1 is engaged in the organization-wide risk framing, the development of the overall C-SCRM strategy, the formation of interdisciplinary groups to engage on C-SCRM, the creation of the organization-wide policies, and a high-level implementation plan to guide C-SCRM activities performed at the mission and business process levels. Level 2 is engaged in developing mission-specific strategies that contextualize the enterprise-level strategy to the specific mission and business processes. Level 2 is also responsible for developing C-SCRM implementation plans that guide strategy implementation within the mission and business processes. C-SCRM activities performed at Level 2 include prioritizing the organization's mission and business processes, and conducting mission/business-level risk assessments, including supply chain risk assessments performed when procuring a product or service. Level 3 is engaged in development of the C-SCRM Plans which guide the application of C-SCRM to specific information systems and information technology acquisitions, including its integration into SDLC processes that guide system development, operation, and maintenance activities. Across the organization, C-SCRM stakeholders coordinate with the various mission and business processes and information system teams to infuse C-SCRM and establish an overarching organizational capability to manage cyber supply chain risks.

[14] Further information about the concepts depicted in Figure 2-2 can be found in [NIST SP 800-39].

Cyber supply chain risk ownership and accountability ultimately lies with the head of the organization:

- The organization's risk profile, risk appetite, and risk tolerance levels will inform who makes risk decisions and processes should address when and how escalation of risk decisions need to occur.
- Ownership should be delegated to authorizing officials within the agency based on their executive authority over organizational missions, business operations or information systems.
- Authorizing officials may further delegate responsibilities to designated officials who are responsible for the day-to-day management of risk.

The C-SCRM activities can be performed by a variety of individuals or groups within an organization ranging from a single individual to committees, divisions, centralized program offices, or any other organizational structures. C-SCRM activities will be distinct for different organizations depending on their organization's structure, culture, mission, and many other factors.

For individual systems, the C-SCRM Plans provide the basis for determining whether an information system meets business, functional, and technical requirements and includes appropriately tailored controls. For missions and business processes, the C-SCRM Strategy and Implementation Plan provides specific C-SCRM activities that lay the foundation for an effective SCRM program and support the achievement of the organization's C-SCRM goals and objectives. The C-SCRM Strategy provides direction and guidance at the enterprise level and should address the integration of C-SCRM considerations into the overall enterprise risk management strategy. C-SCRM Strategy and Implementation Plan(s), and operational-level C-SCRM Plans help organizations focus appropriate resources on the most critical processes and components based on organizational mission/business requirements and their risk environment. Figure 2-3 depicts applicability of different types of C-SCRM documentation to the three risk management framework levels.

These plans are intended to be referenced regularly and should be reviewed and refreshed periodically. These are not intended to be documents developed to satisfy a compliance requirement. Rather, organizations should be able to demonstrate how they have historically and continue to effectively employ their plans to shape, align, inform, and take C-SCRM actions and decisions across all three levels.

Fig. 2-4: C-SCRM Documents in Multi-Level Organization-wide Risk Management

2.1.1. Roles and Responsibilities Across the Three Levels

Implementing C-SCRM requires that organizations establish a coordinated team-based approach to assess cyber supply chain risk and manage this risk by establishing and adhering to policies, developing and following processes (often cross-organizational in nature), as well as employing programmatic and technical mitigation techniques. The coordinated team approach, either ad hoc or formal, enables organizations to more effectively conduct a comprehensive, multi-perspective, analysis of their supply chain and to respond to risks, communicate with external partners/stakeholders, and gain broad consensus regarding appropriate resources for C-SCRM. This team works together to make decisions and take actions that require the input and involvement of multiple perspectives and expertise and leverages, but does not replace those C-SCRM responsibilities and processes that can and should be specifically assigned to an individual organization or disciplinary area. Examples of C-SCRM activities that require a team approach include but are not limited to: developing a strategic sourcing strategy; incorporating C-SCRM requirements into a solicitation; and determining options about how best to mitigate an identified supply chain risk, especially one assessed to be significant.

Members of the C-SCRM team should be a diverse group of people involved in the various aspects of the organization's key processes including but not limited to information security, procurement, enterprise risk management, engineering, software development, IT, legal, and HR. Collectively, to aid in C-SCRM, these individuals should have an awareness of, and provide expertise in, organizational processes and practices specific to their discipline area, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects

and inter-dependencies of systems or information flowing through systems. The C-SCRM team may be an extension of an organization's existing information system risk management, include parts of a general risk management team, or operate out of a different department.

At Level 1, the risk executive functional role is responsible for serving as a common C-SCRM resource for executive leadership and authorizing officials across the organization. Effective C-SCRM requires the risk executive to collaborate and gather perspectives from leaders such as the chief executive officer (CEO), chief risk officer (CRO), chief information officer (CIO), chief legal officer (CLO)/general counsel, chief information security officer (CISO), and chief acquisition officer (CAO). Organizations may form a C-SCRM council to collaborate on setting priorities and managing cyber supply chain risk for the organization. Through the risk framing process, these leaders are responsible for setting the direction for and approving the organization's C-SCRM organization-wide strategy. The C-SCRM strategy makes explicit the organization's assumptions, constraints, risk tolerances, and priorities/trade-offs. These leaders are also responsible for developing and promulgating a holistic set of policies that span the organization's missions and business processes, guiding the establishment and maturation of a C-SCRM capability and the implementation of a cohesive set of C-SCRM activities. Leaders may elect to establish a C-SCRM PMO to drive C-SCRM activities and serve as a fulcrum for coordinated, C-SCRM-oriented services and guidance to the organization. Leaders should also clearly articulate lead roles at the mission and business process level responsible for detailing action plans and being accountable for the execution of C-SCRM activities.

Level 2 roles include but are not limited to representatives of each mission/business process including program managers, research and development, and acquisitions/procurement. Level 2 C-SCRM activities address C-SCRM within the context of the organization's mission and business process. Mission and business process-specific strategies, policies, and procedures should be developed to tailor the C-SCRM implementation to fit the specific requirements of each mission and business process. Aligning to and building off of the high-level Enterprise Strategy and Implementation Plan, the organization should develop its own mission/business-level strategy and implementation plan and ensure C-SCRM execution within the constraints of its defined C-SCRM strategies, as well as awareness of and conformance to its C-SCRM policies. To facilitate the development and execution of Level 2 Strategy and Implementation plan(s), organizations may find benefit in forming a committee with representation from each mission/business process. This coordination and collaboration can help to identify cyber supply chain risks within and across respective mission/business areas and to develop an enterprise and C-SCRM architecture that lends itself to risk-aware mission and business processes. A C-SCRM PMO may also assist in the implementation of C-SCRM at Level 2 through the provision of services (e.g., policy templates, C-SCRM subject matter expert (SME) support).

Level 3 is comprised of personnel responsible for operational activities, including conducting procurements and executing system related C-SCRM activities as part of the organization's SDLC, which includes research and development, design, manufacturing, delivery, integration, operations and maintenance, and disposal/retirement of systems. These personnel include but are not limited to system owners, contracting officers, contracting officer representatives, architects, system integrators, and developers. These personnel are responsible for developing C-SCRM plans which address managing, ensuring the implementation, and monitoring of C-SCRM

controls (to include those applicable to external parties, such as contractors) and the acquisition, development, and sustainment of systems across the SDLC to support mission and business processes. In organizations where a C-SCRM PMO has been established – activities such as product risk assessments may be provided as a centralized shared service.

Table 2-1 shows a summary of C-SCRM stakeholders for each level with the specific C-SCRM activities performed within the corresponding level. These activities are either direct C-SCRM activities or have an impact on C-SCRM.

Table 2-1: Cyber Supply Chain Risk Management Stakeholders

Levels	Level Name	Generic Stakeholder	Activities
1	Organization	Executive Leadership (CEO, CIO, COO, CFO, CISO, Chief Technology Officer (CTO), CRO etc.)	Define Enterprise C-SCRM strategy and high-level implementation plan, policy, goals and objectives
2	Mission	Business Management (includes program management [PM], research and development [R&D], Engineering [SDLC oversight], Acquisition and Supplier Relationship Management/Cost Accounting, and other management related to reliability, safety, security, quality, C-SCRM PMO, etc.)	Develop mission and business process-specific strategy and policies and procedures, guidance and constraints, develop C-SCRM implementation plan(s)
3	Operational	Systems Management (architect, developers, system owner, QA/QC, test, and contracting personnel, approving selection, payment and approach for obtaining, maintenance engineering, disposal personnel, C-SCRM PMO staff, etc.)	Develop C-SCRM plans, implement policies and requirements, adhere to constraints provided by Levels 1 and 2

The C-SCRM process should be carried out across the three risk management levels with the overall objective of continuous improvement in the organization's risk-related activities and effective inter-level and intra-level communication, thus integrating both strategic and tactical activities among all stakeholders with a shared interest in the mission/business success of the organization. Whether addressing a component, a system, a process, a mission process, or a policy, it is important to engage the relevant C-SCRM stakeholders at each level to ensure that risk management activities are as informed as possible.

The next few sections provide example activities in each level. Because each organization is different, however, there may be activities that are performed in different levels than listed as individual organizational context requires.

> Section 4.5 provides a number of mission/business C-SCRM controls that organizations can tailor for their use to help guide Level 1, Level 2, and Level 3 C-SCRM activities. Note the tailoring should be scoped to the organization's risk management needs and organizations should analyze the cost of not implementing C-SCRM policies, capabilities, and controls when evaluating alternative risk response courses of action. These costs may include but are not limited to: poor quality or counterfeit products; supplier misuse of intellectual property; supplier tampering with or compromise of mission-critical information; and exposure to cyber-attacks through vulnerable supplier information systems.

2.1.2. Level 1—Enterprise

Level 1 (Enterprise) sets the tone and direction for organization-wide C-SCRM activities by providing an overarching C-SCRM strategy, C-SCRM policy, and High-Level Implementation Plan that shape how C-SCRM is implemented across the organization. Within Level-1, governance structures are formed to enable senior leaders and executives to collaborate on C-SCRM with the risk executive (function) in which leaders make C-SCRM decisions, delegate decisions to Levels 2 and 3, and prioritize organization-wide resource allocation for C-SCRM. Level 1 activities help to ensure that C-SCRM mitigation strategies are consistent with the strategic goals and objectives of the organization. Level 1 activities culminate in the C-SCRM Strategy, Policy, and High-Level Implementation Plan that shape and constrain how C-SCRM is carried out at Levels 2 and 3.

The C-SCRM governance structures and operational model dictate authority, responsibility, and decision-making power for C-SCRM and define 'how' C-SCRM processes are accomplished within the organization. The best C-SCRM governance and operating model is one that meets business and functional requirements of the organization. For example, an organization facing strict budgetary constraints or stiff C-SCRM requirements may consider governance and operational models which centralize decision-making authority and rely on a C-SCRM PMO to consolidate responsibilities for resource intensive tasks such as vendor risk assessments. In contrast, organizations which have mission/business processes governed with a high degree of autonomy or possess highly differentiated C-SCRM requirements may opt for decentralized authority, responsibilities, and decision-making power.

In addition to defining C-SCRM governance structures and operating models, Level 1 carries out the activities necessary to frame C-SCRM for the organization. C-SCRM framing is the process by which the organization makes explicit the cyber supply chain risk assumptions (e.g., threats, vulnerabilities, risk impact, risk likelihood), constraints (e.g., organization policies, regulations, resource limitation, etc.), appetite and tolerance, and priorities and tradeoffs that guide C-SCRM decisions across the organization. The risk framing process provides the inputs necessary to establish the C-SCRM strategy that dictates how the organization plans to assess, responded to,

and monitor cyber supply chain risk across the organization. A high-level implementation plan should also be developed to guide execution against the organization's C-SCRM strategy. The risk framing process is discussed in further detail within Appendix C of this document.

Informed by the risk framing process and the C-SCRM strategy, Level 1 provides the organization's C-SCRM policy. The C-SCRM policy establishes the C-SCRM program's purpose, outlines the organization's C-SCRM responsibilities, defines and grants authority to C-SCRM roles across the organization, and outlines applicable C-SCRM compliance and enforcement expectations and processes. Appendix C of this document provides example templates for the C-SCRM Strategy and C-SCRM Policy.

Risk assessment activities performed at Level 1 focus on assessing, responding to, and monitoring cyber supply chain risks to the organization's portfolio of operations, assets and personnel. Level 1 risk assessments may be based on the organization's Level 1 Frame step (i.e., assumptions, constraints, appetite, tolerances, priorities and tradeoffs), or may be aggregated enterprise-level assumptions based on risk assessment completed across multiple mission and business processes. For example, a Level 1 risk assessment may analyze the exposure of the organization's primary mission or business objective to a threat scenario affecting a specific product or service provided through the supply chain. The enterprise-level risk determination may be based on an analysis of similar other analyses conducted within several mission and business processes as well as the relative criticality of those processes to the organization's primary objective.

Level 1 activities ultimately provide the overarching context and boundaries within which the organization's mission and business processes manage cyber supply chain risk. Outputs from Level 1 (e.g., C-SCRM Strategy, C-SCRM Policy, Governance and Operating Model) are further tailored and refined within Level 2 to fit the context of each mission and business process. Level 1 outputs should also be iteratively informed by and updated as a result of C-SCRM outputs at lower levels.

Additional information can be found in: SR-1, SR-3, PM-2, PM-6, PM-7, PM-9, PM-28, PM-29, PM-30, and PM-31

2.1.3. Level 2—Mission/Business Process

Level 2 addresses how the organization assesses, responds to, and monitors cyber supply chain risk within mission and business processes. Level 2 activities are performed in accordance with the C-SCRM strategy, and policies provided by Level 1.[15] In this level, process-specific C-SCRM strategies, policies, and implementation plans dictate how the organization's C-SCRM goals and requirements are met within each mission and business process. Here, specific C-SCRM program requirements are defined and managed – including cost, schedule, performance, security, and a variety of critical nonfunctional requirements. These nonfunctional requirements include concepts such as reliability, dependability, safety, security, and quality.

[15] For more information, see [NIST SP 800-39 Section 2.2].

Many threats *to* and *through* the supply chain are addressed at this level in the management of third-party relationships with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Because C-SCRM can both directly and indirectly impact mission and processes, understanding, integrating and coordinating C-SCRM activities at this level are critical for ensuring successful mission and business process operations. Level 2 activities focus on tailoring and applying the organization's C-SCRM frame to fit the specific mission and business process threats, vulnerabilities, impacts, and likelihoods. Informed by outputs from Level 1 (e.g., C-SCRM strategy), mission and business processes will adopt a C-SCRM strategy which tailors the organization's overall strategy to the specific mission and business process. At Level 2, the organization may also issue mission and business process specific policies which contextualize the organization's policy for the process.

In accordance with the C-SCRM strategy, organization leaders for specific mission and business processes should develop and execute a C-SCRM implementation plan. The C-SCRM implementation plan provides a more detailed roadmap for operationalizing the C-SCRM strategy(ies) within the mission and business process. Within the C-SCRM implementation plans, the mission and business process will specify C-SCRM roles and responsibilities, implementation milestones and dates, as well as processes for monitoring and reporting. Appendix D of this document provides example templates for the C-SCRM Strategy and Implementation Plan, as well as the C-SCRM Policy.

C-SCRM activities performed at Level 2 focus on assessing, responding to, and monitoring risk exposure arising from the mission and business process dependencies on suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Risk exposures to the supply chain may arise as a result of primary dependencies on the supply chain or from secondary dependencies of the process on individual information systems or other mission and business processes. For example, risk exposure may arise due to a supplier that provides critical system components or services to multiple information systems that critical processes depend on. Organizations must also consider as a source of risk the products and services unrelated to information systems that vendors provide as well as the role these products and services play in overall mission and business process objectives.

Outputs from Level 2 activities will have a significant impact in shaping how C-SCRM activities are carried out within Level 3. For example, risk tolerance and common control baseline decisions may be defined at Level 2, then tailored and applied within the context of individual information systems within Level 3. Level 2 outputs should also be used to iteratively influence and further refine Level 1 outputs.

Additional information can be found in: SR-1, SR-3, SR-6, PM-2, PM-6, PM-7, PM-30, PM-31, and PM-32.

2.1.4. Level 3—Operational

Within Level 3, outputs provided by C-SCRM activities completed at Levels 1 and 2 prepare the organization to execute C-SCRM at the operational-level in accordance with the RMF [NIST 800-37r2]. C-SCRM is applied to information systems through the development and implementation of C-SCRM plans. These plans are heavily influenced by cyber supply chain risk assumptions, constraints, risk appetite and tolerance, and priorities and tradeoffs defined by Levels 1 and 2. C-SCRM plans dictate how C-SCRM activities are integrated into all systems in the SDLC, which includes acquisition (both custom and off-the-shelf), requirements, architectural design, development, delivery, installation, integration, maintenance, and disposal/retirement. In general, C-SCRM plans are implementation specific, and provide policy implementation, requirements, constraints, and implications for systems that support mission and business process.

Level 3 activities focus on managing operational-level risk exposure resulting from any ICT/OT-related products and services provided through the supply chain that are in use by the organization or fall within the scope of the systems authorization boundary. Level 3 C-SCRM activities begin with an analysis of the likelihood and impact of potential cyber supply chain threats exploiting an operational-level vulnerability (i.e., in a system or system component). Where applicable, these risk assessments should be informed by risk assessments completed in Levels 1 and 2. In response to determined risk, organizations should evaluate alternative courses of action for reducing risk exposure (e.g., accept, avoid, mitigate, share and/or transfer). Risk response is achieved by selecting, tailoring, implementing, and monitoring C-SCRM controls throughout the SLDC in accordance with the RMF [NIST 800-37r2]. Selected C-SCRM controls often consist of a combination of inherited common controls from Levels 1 and 2 as well as information system-specific controls.

A key Level 3 activity is the development of the C-SCRM plan. Along with applicable security control information, the C-SCRM plan includes information on the system, its categorization, operational status, related agreements, architecture, key system personnel, related laws, regulations and policies, and contingency plan. This plan is a living document that should be maintained and used as the reference for continuous monitoring of implemented C-SCRM controls.

Information gathered as part of Level 3 C-SCRM activities should iteratively inform C-SCRM activities completed within Levels 1 and 2 to further refine C-SCRM strategies and implementation plans.

Additional information can be found in: SR-1, SR-2, SR-6, PL-2, PM-31, and PM-32.

2.1.5. C-SCRM PMO

A variety of operating models (e.g., centralized, decentralized, hybrid) are available to organizations that facilitate C-SCRM activities across the organization and its missions/business processes. One such model involves concentrating and assigning responsibilities for certain C-SCRM activities to a central PMO. In this model, the C-SCRM PMO acts as a service provider

to other missions/business processes. Missions/business processes are then responsible for selecting and requesting services from the C-SCRM PMO as part of their responsibilities to meet the organization's C-SCRM goals and objectives. There are a variety of beneficial services that a PMO may provide:

- Advisory services and subject eatter Expertise
- Chair for internal C-SCRM working groups/coordination bodies
- Centralized hub for tools, job aids, awareness and training templates
- Supplier/product risk assessments
- Liaison to external stakeholders
- Information sharing management (e.g., to/from FASC)
- Management of C-SCRM risk register
- Secretariat/staffing function for enterprise C-SCRM governance
- C-SCRM project and performance management
- C-SCRM Briefings, Presentations, and Reporting

A C-SCRM PMO typically consists of C-SCRM SMEs who help drive the C-SCRM strategy and implementation across the organization and its mission and business processes. A C-SCRM PMO may include or report to a dedicated executive-level official responsible for overseeing C-SCRM activities across the organization. Depending on organization-specific constraints, a C-SCRM PMO may consist of dedicated personnel or include matrixed representatives with responsibilities for C-SCRM from several of the organization's processes including, but not limited to information security, procurement, risk management, engineering, software development, IT, legal, and HR.

The C-SCRM PMO responsibilities may include providing services to the organization's leaders that help set the tone for how C-SCRM is applied throughout the organization. The C-SCRM PMO may provide SME support to guide Level 1 stakeholders through the risk framing process which includes establishing the organizational appetite and tolerance for cyber supply chain risk. In addition, accountable risk executives may delegate responsibility for drafting the organization C-SCRM strategy and policy to the PMO. C-SCRM PMOs may also coordinate C-SCRM information-sharing interagency across the supply chain and across the organization mission and business processes. Finally, the PMO may conduct C-SCRM-focused executive-level briefings (e.g., to the risk executive function, board of directors) to help Level 1 stakeholders develop an aggregated picture of the state of cyber supply chain risk across the organization.

At Level 2, C-SCRM PMO may develop C-SCRM starter kits which contain a base strategy, set of policies, procedures and guidelines which can be further customized within specific mission and business processes. This PMO may also provide SME consulting support to stakeholders within mission and business processes as they create process-specific C-SCRM strategies and develop C-SCRM implementation plans. As part of this responsibility, the C-SCRM PMO may advise on or develop C-SCRM common control baselines within the organization mission and business processes. The C-SCRM PMO may also perform C-SCRM risk assessments focused on suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers of both technology and non-technology related products and services.

The responsibility of a C-SCRM PMO at Levels 1 and 2 would ultimately influence C-SCRM activities at the Level 3 operational level. A C-SCRM PMO may advise teams throughout the SDLC on C-SCRM control selection, tailoring, and monitoring. Ultimately a C-SCRM PMO may be responsible for activities that produce C-SCRM outputs across the risk management levels. Centralizing C-SCRM services offers organizations an opportunity to capitalize on specialized skill sets within a consolidated team that offers high quality C-SCRM services to the rest of the organization. By centralizing risk assessment services – organizations may achieve a level of standardization not otherwise possible (e.g., in a decentralized model). Organizations may also realize cost efficiencies in cases where PMO resources are dedicated to C-SCRM activities versus resources in decentralized models which may perform multiple roles in addition to C-SCRM responsibilities.

3. CRITICAL SUCCESS FACTORS

To successfully address evolving cyber supply chain risks, organizations need to engage multiple internal processes and capabilities, communicate and collaborate across organizational levels and mission areas, and ensure that all individuals within the organization understand their role in managing cyber supply chain risks. Organizations need strategies for communicating, determining how best to implement, and monitoring the effectiveness of their supply chain cybersecurity controls and practices. In addition to communicating cyber supply chain controls internally, organizations should engage with peers to exchange cyber supply chain risk management insights. These insights will aid organizations in continuously evaluating how well they are doing and identify where they need to improve and how to take steps to mature their C-SCRM program. This section addresses the requisite organizational processes and capabilities to make C-SCRM successful.

3.1. C-SCRM in Acquisition

Integrating C-SCRM considerations into acquisition activities is essential to improving management of cyber supply chain risks at every step of the procurement and contract management process. This life cycle begins with a purchaser identifying a need, includes the processes to plan for and articulate requirements, conduct research to identify and assess viable sources of supply, solicit bids and evaluate offers, to include ensuring conformance to C-SCRM requirements and assessing C-SCRM risk associated with the bidder and the proposed product and/or service offering. After contract award, ensure the supplier satisfies the terms and conditions articulated in their contractual agreement and that the products and services conform as expected and required. C-SCRM considerations need to be addressed at every step in this life cycle.

Organizations rely heavily on commercial products and outsourced services to perform operations and fulfill their missions and business objectives. In addition to addressing cyber supply chain risks and performing C-SCRM activities during each phase of the acquisition process, organizations should develop and execute an acquisition strategy that drives forward reductions in their overall cyber supply chain risk exposure. Through such strategies, organizations can reduce cyber supply chain risks within specific procurement processes as well as for the overall enterprise. Adopting acquisition policies and processes that integrate C-SCRM will then aid, direct, and inform the organization's efforts to implement those strategies and realize targeted risk-reducing outcomes which align and lead to achievement of the organization's C-SCRM strategic goals and objectives.

Additionally, adopting C-SCRM controls aligned to an industry-recognized set of standards and guidelines (e.g., NIST 800-53 Rev.5, NIST CSF), the organization can ensure holistic coverage of cyber supply chain risks and corresponding C-SCRM practices. C-SCRM controls may apply to different participants of the supply chain to include the organization itself, prime contractors, and sub-contractors. Because organizations heavily rely on prime contractors and their subcontractors to develop and implement ICT products and services, those controls that are implemented within the SDLC are likely to flow down to subcontractors. Establishing C-SCRM controls that apply throughout the supply chain and the SDLC will aid the organization in

establishing common expectations and lexicon with suppliers and sub-suppliers to help all participants manage cyber supply chain risks to and through the supply chain.

3.1.1. Acquisition in the C-SCRM Strategy and Implementation Plan

An organization's C-SCRM Strategy and Implementation Plan serve as the roadmap to guide the organization toward achievement of long-term, sustainable reductions in cyber supply chain risk exposure. As a core part of the C-SCRM Strategy and Implementation Plan, organizations should address how cyber supply chain risks are managed throughout the acquisition process.

Cyber supply chain risks include those arising from the supplier's organization, products or services, as well as the supplier's own suppliers and supply chains. The C-SCRM PMO may be helpful in developing specific strategies and implementation plans for integrating C-SCRM considerations into acquisitions. Acquisition activities relevant to C-SCRM include, but are not limited to:

- Promoting awareness and communicating C-SCRM expectations as part of supplier relationship management efforts;
- Establishing a checklist of acquisition security requirements that must be completed as part of procurement requests to ensure necessary provision and protections are in place;
- Leveraging an external shared service provider or utilize the C-SCRM PMO to provide supplier, product, and/or services assessment activities as a shared service to other internal processes including acquisition;
- Conducting robust due diligence to inform determinations about a bidder's responsibility and to identify and assess bidders' cyber supply chain risk posture or risk associated with a given product or service offering;
- Including C-SCRM criteria in source selection evaluations;
- Establishing and referencing a list of prohibited suppliers, if appropriate, per applicable regulatory and legal references; and
- Establishing and procuring from an approved products list or list of preferred or qualified suppliers who have demonstrated conformance with the organization's security requirements through a rigorous process defined by the organization or another acceptable qualified list program activity.

The C-SCRM Strategy and Implementation Plan should address the acquisition security-relevant foundational elements necessary to implement a C-SCRM program. To support the strategy, organization leaders should promote the value and importance of C-SCRM within acquisitions and ensure sufficient, dedicated funding is in place for necessary activities. Doing so will help organizations ensure responsibility for program processes and accountability for progress toward the attainment of results. Organizations should also assign roles and responsibilities, some of which will be cross-organizational in nature and team-based, while others will be specific to acquisition processes. Finally, relevant training should be provided to members of the acquisition workforce to ensure roles and responsibilities are understood and executed in alignment with leader expectations.

The organization's capabilities, resources, operational constraints and existing portfolio of supplier relationships, contracts, acquired services and products provide the baseline context necessary to lay out a strategic path that is realistic and achievable. This baseline starting point also serves as a marker from which performance progress and outcomes can be tracked and assessed.

A critical first step is to ensure there is a current and accurate inventory of the organization's supplier relationships and contracts as well as an understanding of the products or services those suppliers provide. This information allows for a mapping of these suppliers into strategically relevant groupings. For example, an assessment of these suppliers might result in a grouping of them into categories (e.g., "strategic/innovative," "mission-critical," "sustaining" or "standard/non-essential"). This segmentation facilitates further analysis and understanding of the exposure to cyber supply chain risk throughout the organization, and helps to focus priority attention on those critical suppliers that are of the most strategic or operational importance to the organization and its mission and business processes. It is useful to identify which products and services require a higher level of confidence that risk is minimized, and can be helpful in identifying areas of risk, such as overreliance on a single source of supply. This inventory and mapping also facilitates the selection and tailoring of C-SCRM contract language and evaluation criteria.

Additional information can be found in: SA-1, SA-2, SA-4, SR-5, SR-13, and NISTIR 8179[1]

3.1.2. The Role of C-SCRM in the Acquisition Process

When conducting a procurement, organizations should designate experts from different subject matter areas to participate in the acquisition process as members of the Acquisition Team. While procurement requirements address and are tailored to satisfying a specific purpose and ensure compliance mandates are met, contextual factors such as mission criticality, sensitivity of data, and the operational environment must also be considered to effectively address cyber supply chain risk.

This contextual basis sets the stage for the Acquisition Team to be able to effectively gauge their tolerance for risk as it pertains to a specific procurement requirement and determine which of the [NIST SP 800-161 Rev 1] and [NIST SP 800-53 Rev 5] controls are relevant and necessary to consider for specific acquisitions. The program office – or requiring official – should consult with information security personnel to complete this control selection process and work with their procurement official to incorporate these controls into requirements documents and contracts. Security is a key factor in procurement decisions.

Acquisition policies and processes need to incorporate C-SCRM considerations into each step of the procurement and contract management life cycle management process (i.e., plan procurement, define/develop requirements, perform market analysis, complete procurement, ensure compliance, monitor performance and for changes that affect C-SCRM risk status) as described in [NISTIR 7622]. During the 'plan procurement' step, the criticality of the good or service to be procured needs to be identified, along with a description of the factors that are driving the determination of the level of criticality. This activity is typically led by the

procurement official with the help from officials across the organization including but not limited to mission/business representatives, information security, and legal.

Once a procurement plan is in place, the organization should develop and define requirements. Requirements should be developed and refined to address cyber supply chain risks, in addition to specifying performance, schedule, and cost objectives. This process is typically initiated by the acquirer mission/business process owner or a designee in collaboration with the procurement official and other members of the C-SCRM team.

With requirements defined, organizations will typically complete a market analysis for potential suppliers. Market research and analysis activities will explore the availability of potential or pre-qualified sources of supply. This step is typically initiated by the acquirer mission and business process owner or a designated representative. Organizations should use this phase to conduct more robust due diligence research on potential suppliers and/or products in order to generate a supplier risk profile. As part of due diligence, the organization may consider the market concentration for the sought-after product or service as a means of identifying interdependencies within the supply chain. The organization may also use a request for information (RFIs) and/or due diligence questionnaires for the initial screening and collection of evidence from potential suppliers. Organizations should not treat the initial C-SCRM due diligence risk assessment as exhaustive. Results of this research can also be helpful in shaping the sourcing approach and refining requirements.

Finally, the organization will complete the procurement step by releasing a statement of work (SOW) or statement of objective (SOO) for the release of a request for proposal (RFP), or request for quotes (RFQ). As part of selection, any bidders responding to the RFP or RFQ should be evaluated against relevant, key C-SCRM criteria. The RFP review process should also include any procurement-specific supplier risk assessment. The assessment criteria will be heavily informed by the defined C-SCRM requirements and include coverage over but not limited to information about the organization, its security processes, and its security track record. The response review process involves multiple C-SCRM stakeholders including procurement, the mission and business process owner, as well as appropriate information system owners and technical experts. Once selection has occurred, organizations should complete product or system component risk assessments with coverage over, but not limited to the products or system components quality, vulnerability, and authenticity.

Once the contract is executed, the organization should monitor for change that alters its cyber supply chain risk exposure. Change that alters cyber supply chain risk exposure may include but is not limited to internal organization or system changes, supplier operational or structural changes, as well as geopolitical or environmental changes. An organization should continuously apply lessons learned collected during the acquisition process to enhance its ability to assess, respond to and monitor cyber supply chain risk within its supply chain.

Table 3-1 shows a summary of where C-SCRM assessments may take place within the various steps of the procurement process.

1706 **Table 3-1: C-SCRM in the Procurement Process**

Procurement Process	Service Risk Assessment	Supplier Risk Assessment	Product Risk Assessment
Plan Procurement	Service Risk Assessment Criticality of Needed Service Other Context (functions performed; access to systems/data, etc.) Fit for Purpose	Fit for Purpose	Criticality of Needed Product Other Context (Operating Environment, Data, Users, etc.) Fit for Purpose
Define/Develop Requirements	Select applicable C-SCRM controls/ requirements	Select applicable C-SCRM controls/ /requirements	Select applicable C-SCRM controls/ requirements
Perform Market Analysis		Initial Risk Assessment (e.g., Due-Diligence Questionnaires)	Research product options and risk factors
Solicit Bids/ Complete Procurement		Complete Risk Assessment	Pre-Deployment Risk Assessment
Operate & Maintain	Continuous Risk Monitoring	Continuous Risk Monitoring	Continuous Risk Monitoring

1707

1708 In addition to process activities, there are many useful acquisition security-enhancing tools and
1709 techniques available, including: obscuring the end use of a system or system component; using
1710 blind or filtered buys; requiring tamper-evident packaging; or using trusted or controlled
1711 distribution. The results from a supply chain risk assessment can guide and inform the strategies,
1712 tools, and methods that are most applicable to the situation. Tools and techniques may provide
1713 protections against unauthorized production, theft, tampering, insertion of counterfeits, insertion
1714 of malicious software or backdoors, and poor development practices throughout the system
1715 development life cycle.

1716 To ensure effective and continued management of cyber supply chain risks throughout the
1717 acquisition lifecycle, contractual agreements and contract management should include:
1718 • The satisfaction of applicable security requirements in contracts and mechanisms as a
1719 qualifying condition for award;
1720 • Flow-down control requirements to sub-contractors, if and when applicable, including C-
1721 SCRM performance objectives, linked to method of inspection, in a Quality Assurance
1722 Surveillance Plan;
1723 • Periodic re-validation of supplier adherence to security requirements to ensure continual
1724 compliance;
1725 • Processes and protocols for communication and reporting of information about
1726 vulnerabilities, incidents, and other business disruptions, to include acceptable deviations if
1727 the business disruption is serious enough and baseline criteria to determine whether a
1728 disruption qualifies as serious ; and
1729 • Terms and conditions that address government, supplier, and other applicable third
1730 party(ies) roles, responsibilities, and actions for responding to identified supply chain

risk(s), or risk incident(s), in order to mitigate risk exposure, minimize harm, and support timely corrective action or recovery from an incident.

There are a variety of acceptable validation and re-validation methods, such as required certifications, site visits, third-party assessment, or self-attestation. The type and rigor of required methods should be commensurate to the criticality of the service or product being acquired and the corresponding assurance requirements.

Additional guidance for integrating C-SCRM into the acquisition process is provided in Appendix C that demonstrates the enhanced overlay of C-SCRM into the NIST SP 800-39 Risk Management Process. In addition, organizations should refer to and follow acquisition/procurement policies, regulations, and best practices that are specific to their domain (e.g., critical infrastructure sector, State Government, etc.)

Additional information can be found in: SA-1, SA-2, SA-3, SA-4, SA-9, SA-19, SA-20, SA-22, SR-5, SR-6, SR-10, and SR-11

3.2. Supply Chain Information Sharing

Organizations are continuously exposed to risk originating from their supply chains. An effective information-sharing process helps to ensure organizations can gain access to information critical to understanding and mitigating cyber supply chain risks, and also share relevant information to others that may benefit from or require knowing about these risks.

To aid in identifying, assessing, monitoring, and responding to cyber supply chain risks, organizations should build information-sharing processes and activities into their C-SCRM programs. This may include establishing information-sharing agreements with peer organizations, as well as with business partners and suppliers. By exchanging supply chain risk information within a sharing community, organizations can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats the organization may face. Additionally, sharing of supply chain risk information allows organizations to better detect campaigns that target specific industry sectors and institutions.

Federal organizations should establish processes to be able to effectively engage with the FASC's information sharing agency, which is responsible for facilitating information sharing among government agencies and acts as a central, government-wide facilitator for C-SCRM information sharing activities.

NIST SP 800-150 describes key practices for establishing and participating in supply chain risk information-sharing relationships as follows:

- Establish information sharing goals and objectives that support business processes and security policies
- Identify existing internal sources of supply chain risk information
- Specify the scope of information sharing activities
- Establish information sharing rules

- Join and participate in information sharing efforts
- Actively seek to enrich indicators by providing additional context, corrections, or suggested improvements
- Use secure, automated workflows to publish, consume, analyze, and act upon supply chain risk information
- Proactively establish supply chain risk information sharing agreements
- Protect the security and privacy of sensitive information
- Provide ongoing support for information sharing activities.

As shown in Table 3-2, below, supply chain risk information describes or identifies cyber supply chain relevant characteristics and risk factors associated with a product or service or source of supply. It may exist in various forms (e.g., raw data, a supply chain network map, risk assessment report, etc.) and should be accompanied with the metadata that will facilitate an assessment of a level of confidence in and credibility of the information. Organizations should follow established processes and procedures that describe whether and when sharing or reporting of certain information is mandated or voluntary and if there are any necessary requirements with which to adhere regarding information handling, protection and classification.

1792 **Table 3-2: Cyber Supply Chain Characteristics and Risk Factors Associated with a**
1793 **Product, Service, or Source of Supply[16]**

Source of Supply, Product, or Service Characteristics	Risk Indicators, Analysis, and Findings
• Features and functionality; • Access to data and information, including system privileges; • Installation or Operating Environment; • Security, authenticity, and integrity of a given product or service and the associated supply and compilation chain; • The ability of the source to produce and deliver a product or service, as expected; • Foreign control of, or influence over, the source (e.g., foreign ownership, personal and professional ties between the source and any foreign entity, legal regime of any foreign country in which the source is headquartered or conducts operations); • Market alternatives to the source; and • Potential risk factors such as geo-political, legal, managerial/internal controls, financial stability, cyber incidents, personal and physical security, or any other information that would factor into an analysis of the security, safety, integrity, resilience, reliability, quality, trustworthiness, or authenticity of a product, service or source.	• Threat information include indicators (system artifacts or observables associated with an attack), tactics, techniques, and procedures (TTPs); • Security alerts, threat intelligence reports; • Implications to national security, homeland security, and/or national critical processes associated with use of the product or service; • Vulnerability of federal systems, programs, or facilities; • Threat level and vulnerability level assessment/score; • Potential impact or harm caused by the possible loss, damage, or compromise of a product, material, or service to an organization's operations or mission and likelihood of a potential impact or harm, or the exploitability of a system; and • Capacity to mitigate risks identified.

1794
1795
1796 ## 3.3. C-SCRM Training and Awareness
1797
1798 Numerous individuals within the organization contribute to the success of C-SCRM. These may
1799 include but are not limited to information security, procurement, risk management, engineering,
1800 software development, IT, legal, HR. Examples of these contributions include:

[16] Cyber Supply Chain Characteristics and Risk Factors Associated with a Product, Service, or Source of Supply is non-exhaustive.

- System Owners are responsible for multiple facets of C-SCRM at the operational-level as part of their responsibility for the development, procurement, integration, modification, operation, maintenance, and/or final disposition of an information system;
- Human Resources defines and implements background checks and training policies which help ensure that individuals are trained in appropriate C-SCRM processes and procedures;
- Legal helps draft C-SCRM-specific contractual language that is included by procurement in contracts with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers;
- Acquisition/procurement defines the process for implementing supplier assurance practices embedded in the acquisition process;
- Engineering designs products and must understand existing requirements for use of open-source components;
- Software developers ensure software vulnerabilities are identified and addressed as early as possible, including testing and fixing the code;
- Shipping and receiving ensures that boxes that contain critical components have not been tampered with en route or at the warehouse.

Everyone within an organization has a role in managing cyber supply chain risks. The organizations should foster an overall culture of security including C-SCRM as an integral part. The organizations can use a variety of communication methods to foster the culture, of which traditional awareness and role-based training are only one component.

Every individual within an organization should receive appropriate training to help them understand the importance of C-SCRM for their organization, their specific roles and responsibilities, and processes and procedures for reporting incidents. This training can be integrated into the overall cybersecurity awareness training.

Those individuals who have more significant roles in managing cyber supply chain risk should receive tailored C-SCRM training that helps them understand the scope of their responsibilities, specific processes and procedures they are responsible for implementing, and what actions to take in case of an incident, disruption, or another C-SCRM-related event. The organizations should establish specific role-based training criteria and develop role-specific C-SCRM training to address specific C-SCRM roles and responsibilities. The organizations may also consider adding C-SCRM content into already existing role-based training for some specific roles. Refer to the Awareness and Training controls in Section 4.5 for more detail.

Organizations should consider use of the NIST National Initiative for Cybersecurity Education (NICE) Framework[17] as a means of forming a common lexicon on C-SCRM workforce topics. This will aid organizations in developing training linked to role-specific C-SCRM responsibilities and communicating cybersecurity workforce-related topics. The NICE Framework outlines Categories, Specialty Areas, Work Roles, KSAs (Knowledge, Skills, and Abilities), and Tasks which describe cybersecurity work.

[17] NIST Special Publication 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

3.4. Capability Implementation Measurement and C-SCRM Metrics

Organizations should actively manage the efficiency and effectiveness of their C-SCRM programs through ongoing measurement of the programs themselves. Organizations can use several methods of measuring and managing the effectiveness of their C-SCRM program:

- Using a framework, such as NIST CSF to assess their C-SCRM capabilities
- Measuring progress of their C-SCRM initiatives towards completion
- Measuring performance of their C-SCRM initiatives towards desired outcomes

All methods rely on a variety of data collection, analysis, contextualization, and reporting activities. Collectively, these methods should be used to track and report out progress and results that ultimately indicate reductions in risk exposure and improvements in the organization's security outcomes.

C-SCRM performance management provides a number of organizational and financial benefits. Major benefits include increasing stakeholder accountability for C-SCRM performance; improving effectiveness of C-SCRM activities; demonstrating compliance with laws, rules and regulations, providing quantifiable inputs for resource allocation decisions, cost-avoidance associated with reduced impact from—or likelihood of experiencing—a cyber-supply chain incident.

Organizations can use a framework such as NIST CSF Implementation Tiers to baseline their C-SCRM capabilities. Frameworks such as this provide a useful context for an organization to track and gauge the increasing rigor and sophistication of their C-SCRM practices. Progression against framework topics is measured using ordinal (i.e., 1-5) scales which illustrate the progression of capabilities across tiers. The following are examples of how C-SCRM capability could be gauged by applying NIST CSF Tiers:

- CSF Tier 1: The organization does not understand its cyber supply chain risks or its role in the larger ecosystem. The organization does not collaborate with other entities or have processes in place to identify, assess and mitigate its cyber supply chain risks.

- CSF Tier 2: The organization understands its cyber supply chain risks associated with products and services and its role in the larger ecosystem. The organization has not formalized its capabilities to manage cyber supply chain risks internally or its capability to engage and share information with entities in the broader ecosystem.

- CSF Tier 3: Organization-wide approach to managing cyber supply chain risks is enacted via enterprise risk management policies, processes, and procedures. This likely includes a governance structure (e.g., Risk Council) that manages cyber supply chain risks in balance with other enterprise risks. Policies, processes, and procedures are implemented consistently, as intended, and continuously monitored and reviewed. Personnel possess the knowledge and skills to perform their appointed cyber supply chain risk management responsibilities. The organization has formal agreements in place to communicate baseline requirements to its suppliers and partners. The organization understands its external dependencies and collaborates with partners to share information to enable risk-

based management decisions within the organization in response to events.

- CSF Tier 4: The organization actively consumes and distributes information with partners and uses real-time or near real-time information to improve cybersecurity and supply chain security before an event occurs. The organization leverages institutionalized knowledge of cyber supply chain risk management with its external suppliers and partners as well as internally, in related functional areas and at all levels of the organization. The organization communicates proactively using formal (e.g., agreements) and informal mechanisms to develop and maintain strong relationships with its suppliers, buyers, and other partners.

Capability building begins by establishing a solid programmatic foundation that includes enabling strategies and plans, policies and guidance, investment in training and dedicated program resources. Once this foundational capability is in place, organizations can use these progression charts to orient the strategic direction of their programs to target states of C-SCRM capability in different areas of the program. Table 3-3 provides an example C-SCRM implementation model.

1898

1899 **Table 3-3: Example C-SCRM Practice Implementation Model[18]**

Implementation Level	Associated C-SCRM Practices
Foundational	• Established C-SCRM Policies across enterprise-levels • Defined C-SCRM hierarchy • Established C-SCRM governance structure • Well-documented, consistent C-SCRM processes • Quality and reliability program • Explicit roles for C-SCRM • Adequate and dedicated C-SCRM resources • Defined C-SCRM control baseline • Established C-SCRM internal checks and balance to assure compliance • Established supplier management program • C-SCRM included in an established incident management program
Sustaining	• Use of third-party assessments, site visits, and formal certification • Defined C-SCRM risk appetite and risk tolerances • Formalized information sharing processes (e.g., engages w/ FASC) • Formal C-SCRM training program • C-SCRM integrated into SDLC • C-SCRM integrated into contractual agreements • Suppliers participate in incident response, disaster recovery, and contingency planning • Formally defined, collected, and reported C-SCRM metrics
Enhancing	• C-SCRM process automation • Use of quantitative risk analysis • Predictive and adaptive C-SCRM strategies and processes

1900

1901 ### 3.4.1. Measuring C-SCRM Efficacy, Efficiency, and Compliance

1902

1903 Organizations typically rely on information security measures to facilitate decision making as
1904 well as improve performance and accountability in their information security programs.
1905 Organizations can achieve similar benefits within their C-SCRM programs. Similar to
1906 information security measures, C-SCRM-focused measures can be obtained at different levels of
1907 an organization. NIST SP 800-55 provides guidance on the specific development, selection, and
1908 implementation of operational-level and program-level performance measures. Table 3-3
1909 provides example measurement topics across the three Risk Management levels.

[18] For more information on C-SCRM capabilities, refer to section 1.5 C-SCRM Key Practices.

1910 **Table 3-4: Example Measurement Topics Across the Risk Management Levels**

Risk Level	Example Measurement Topics
Level 1	• Policy adoption at lower levels • Timeliness of policy adoption at lower levels • Adherence to risk appetite and tolerance thresholds • Differentiated levels of risk exposure across Level 2 • Compliance with regulatory mandates • Adherence to customer requirements
Level 2	• Effectiveness of mitigation strategies • Time allocation across C-SCRM activities • Mission/business process-level risk exposure • Degree and quality of C-SCRM requirement adoption in mission/business processes • Use of C-SCRM PMO by Level 3
Level 3	• Design effectiveness of controls • Operating effectiveness of controls • Cost-efficiency of controls

1911

1912 Organizations may adopt a single or combination of methods to manage the effectiveness of their
1913 C-SCRM programs. NIST SP 800-55 Rev.1 articulates three different components of
1914 performance:

1915 • **Implementation:** Demonstrates the progress in implementing programs, controls, and
1916 associated policies and procedures;
1917 • **Effectiveness/Efficiency:** Provides insight whether programs, processes, and controls are
1918 implemented correctly, operate as intended, and meet desired outcomes;
1919 • **Impact:** Analyzes the impact of C-SCRM on broader objectives (e.g., contribution to
1920 business process cost savings; reduction in national security risk).

1921 ## 3.5. Dedicated Resources
1922

1923 To appropriately manage cyber supply chain risks, organizations should commit dedicated funds
1924 towards this effort. Identifying resource needs and taking steps to secure adequate, recurring, and
1925 dedicated funding is an essential and important activity that needs to be built into the C-SCRM
1926 strategy and implementation planning effort and incorporated into an organization's budgeting,
1927 investment review, and funds management processes. Access to adequate resources is a critical,
1928 key enabler for the establishment and sustainment of a C-SCRM program capability. The
1929 continued availability of dedicated funds will allow organizations to sustain, expand, and mature
1930 their capabilities over time.
1931

Securing and assigning C-SCRM funding is representative of leadership's commitment to the importance of C-SCRM and its relevance to national and economic security and ensuring the protection, continuity and resilience of mission and business processes and assets.

Funding facilitates goal and action-oriented planning. Examining resource needs and allocating funding prompts a budgeting and strategic planning process. Effective organizations begin by defining a set of goals and objectives upon which organizations should build a strategic roadmap laying out the path to achieve them, through the assignment and allocation of finite resources. The establishment of dedicated funding, tied to C-SCRM objectives, sets conditions for accountability for performance and compels responsible staff to be efficient and effective and to adopt a mindset of continuously seeking to improve C-SCRM capabilities and achieve security enhancing outcomes.

Obtaining new or increased funding can be a challenge as resources are often scarce and necessary for many competing purposes. The limited nature of funds forces prioritization. C-SCRM leaders need to first examine what can be done within the constraints of existing resources and be able to articulate, prioritize, and defend their requests for additional resources. For new investment proposals, this requires a reconciliation of planned initiatives against the organization's mission/business objectives. When well-executed, a systematic planning process can tighten the alignment of C-SCRM processes to these objectives.

Many C-SCRM processes can and should be built into existing program and operational activities and may be able to be adequately performed using available funds. However, there may be a need for an influx of one-time resources to establish an initial C-SCRM program capability. For example, this might include the need to hire new personnel with expertise in C-SCRM, to acquire contractor support to aid in developing C-SCRM program guidance, or to develop content for role-based C-SCRM training. There may also be insufficient resources in place to satisfy all recurring C-SCRM program needs. Existing funds may need to be reallocated towards C-SCRM efforts or new or additional funds requested. Organizations should also seek out opportunities to leverage shared services whenever practical.

The use of shared services can optimize the use of scarce resources and concentrates capability into centers of excellence providing cost-efficient access to services, systems, or tools. Organizations pursuing shared service models for C-SCRM should also be aware of the challenges with such models. Shared services (e.g., C-SCRM PMO) are most effective when the organization at large relies on a fairly homogenous set of C-SCRM strategy, policies, and processes. In many instances, centralized delivery of C-SCRM services require a robust technology infrastructure. The organization's systems should be able to support process automation and centralized delivery in order to fully realize the benefits of a shared services model.

Consultation with budget officials is critical to understanding what options may be available and viable in the near term and outyears. These officials can also advise on how best to justify needs, and the timeframes and processes for requesting new funds. There are likely different processes to follow for securing recurring funds, as compared with requesting one-time funding. For example, funding for a new information system to support a C-SCRM capability may involve the

development of a formal business case that must be presented to an organization's investment review board for approval. Breaking out resource needs into ongoing and one-time costs, as well as into cost categories that align with budget formulation, resource decision-making, and the allocation and management of available funds will also be helpful.

It is recommended that the C-SCRM PMO have the lead responsibility of coordinating with mission/business process and budget officials to build out and maintain a multi-year C-SCRM program budget that captures both recurring and non-recurring resource requirements and maps those requirements to available funding and fund sources. To understand what amount of funding is required, at what time, and for what purpose, organizations should identify and assess which type and level of resources (people or things), are required to implement a C-SCRM program capability and perform required C-SCRM processes on an ongoing basis. The costs associated with each of these identified resource needs would then be captured, accumulated, and reflected in a budget that includes line items for relevant cost categories, such as personnel costs, contracts, training, travel, or tools and systems. This will provide the organization a baseline understanding of what can be accomplished within existing resource levels and where there are gaps in need of being filled. The actual allocation of funds may be centralized in a single C-SCRM budget or may be dispersed across the organization and reflected in individual office or mission/business process-area budgets. Regardless of how funds are actually assigned, having a centralized picture of the C-SCRM budget and funds status will serve as a valuable source of information that justify new requests, inform prioritization decisions and adjust expectations about certain activities and the duration in which they can be accomplished.

Ensuring C-SCRM program funding is distinctly identified within the organization's budget—with performance measures linked to the funding—will drive accountability for results. The visible dedication of funds in budget requests and performance plans and reports compels leadership attention on C-SCRM processes and accomplishment of objectives. Budgets must be requested and justified on a periodic basis and this process allows leadership and oversight officials to trace and measure the effectiveness and efficiency of allocated resources. This, in turn, serves as a driving function for program and operational C-SCRM personnel to track and manage their performance.

4. C-SCRM CONTROLS

NIST defines security controls as:

> *The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [FIPS 200, FIPS 199, CNSSI No. 4009, NIST SP 800-37 Rev. 1, NIST SP 800-53 Rev. 5, NIST SP 800-53A Rev. 5]*

NIST SP 800-53 Rev. 5 defines numerous cyber supply chain-related controls within the catalog of information security controls. This section is structured as an enhanced overlay of NIST SP 800-53 Rev. 5. It identifies and augments C-SCRM-related controls with additional supplemental guidance and provides new controls as appropriate. The C-SCRM controls are organized into the twenty (20) control families of NIST SP 800-53 Rev. 5. This approach facilitates use of the security controls assessment techniques provided in NIST SP 800-53A Rev. 5 to assess implementation of C-SCRM controls.

The controls provided in this publication are intended for organizations to implement internally, as well as require of their contractors and subcontractors, if and when applicable, and as incorporated into a contractual agreement. As with NIST SP 800-53 Rev. 5, the security controls and control enhancements are a starting point from which controls/enhancements may be removed, added, or specialized based on an organization's needs. Each control in this section is listed for its applicability to C-SCRM. Those controls from NIST SP 800-53 Rev. 5 not listed are not considered directly applicable to C-SCRM, and thus are not included in this publication. Details and supplemental guidance for the various C-SCRM controls in this publication are contained in Section 4.5.

4.1 C-SCRM CONTROLS SUMMARY

During the Respond Step of the risk management process discussed in Section 2, organizations select, tailor, and implement controls for mitigating cyber supply chain risk. NIST 800-53B lists a set of information security controls at the FIPS 199 high-, moderate-, and low-impact levels. This section describes how these controls help mitigate risk to information systems and components, as well as the cyber supply chain infrastructure. The section provides twenty (20) C-SCRM control families that include relevant controls and supplemental guidance.

Figure 4-1 depicts the process used to identify, refine, and add C-SCRM supplemental guidance to the NIST SP 800-53 Rev. 5 C-SCRM-related controls. The figure, which repeats Figure 1-5, represents the following steps:

1. Selected and extracted individual controls and enhancements from NIST SP 800-53 Rev. 5 that were applicable to C-SCRM;
2. Analyzed these controls to determine how they apply to C-SCRM;
3. Evaluated the resulting set of controls and enhancements to determine whether all C-SCRM concerns were addressed;

4. Developed additional controls currently not defined in NIST SP 800-53 Rev. 5;
5. Identified controls for flow down to relevant sub-level contractors;
6. Assigned applicable levels to each C-SCRM control; and
7. Developed C-SCRM-specific supplemental guidance for each C-SCRM control.

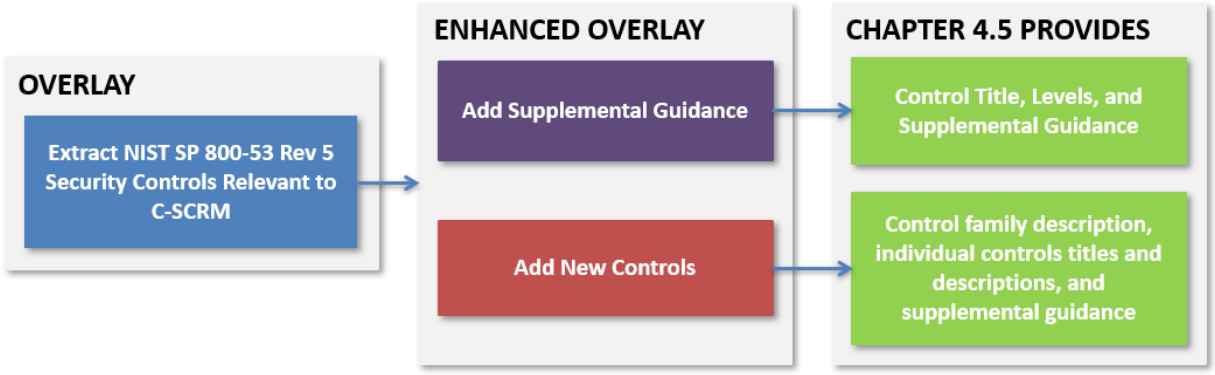


Fig. 4-1: C-SCRM Security Controls in NIST SP 800-161 Revision 1, Section 4.5

Note that NIST SP 800-53 Rev. 5 provides C-SCRM-related controls and control families. These controls may be listed in this publication with a summary or additional guidance and a reference to the original NIST SP 800-53 Rev. 5 control and supplemental guidance detail.

4.2 C-SCRM CONTROLS THROUGHOUT THE ORGANIZATION

As noted in Table 4-1, C-SCRM controls in this publication are designated by the three levels comprising the organization. This is to facilitate C-SCRM control selection specific to organizations, their various missions, and individual systems, as described in Appendix C under the Respond step of the risk management process. During controls selection, organizations should use the C-SCRM controls in this section to identify appropriate C-SCRM controls for tailoring, per risk assessment. By selecting and implementing applicable C-SCRM controls for each level, organizations will ensure that they have appropriately addressed C-SCRM throughout their organizations.

4.3 APPLYING C-SCRM CONTROLS TO ACQUIRING PRODUCTS AND SERVICES

Acquirers may use C-SCRM controls as the basis from which to communicate their C-SCRM requirements to different types of organizations, described within this publication, that provide products and services to acquirers, including suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Acquirers should avoid using generalized requirements statements, such as “ensure compliance with NIST SP 800-161 Rev. 1 controls.” Acquirers must be careful to select the controls relevant to the specific use case of the service or product being acquired. Acquirers are encouraged to integrate C-SCRM

2089 throughout their acquisition activities. More details on the role of C-SCRM in acquisition is
2090 provided in Section 3.1 of this document.
2091
2092 It is important to recognize the controls in this section do not provide specific contracting
2093 language. Acquirers should develop their own contracting language using this publication as
2094 guidance to develop specific C-SCRM requirements for inclusion in contracts. The following
2095 sections expand upon the supplier, developer, system integrator, external system service
2096 provider, and other ICT/OT-related service provider roles with respect to C-SCRM expectations
2097 for acquirers.
2098
2099 Organizations may use multiple techniques to ascertain w these controls are in place. Techniques
2100 may include supplier self-assessment, acquirer review, or third-party assessments for
2101 measurement and conformance to the organization's requirements. Organizations should first
2102 look to established third-party assessments to see if they meet their needs. When an organization
2103 defines C-SCRM requirements, it may discover that established third-party assessments may not
2104 address all specific requirements. In this case, additional evidence may be needed to justify
2105 additional requirements. Please note that the data obtained for this purpose should be
2106 appropriately protected.
2107
2108 ***4.3.1 Suppliers***

2109 Suppliers may provide either commercial off-the-shelf (COTS) or, in federal contexts,
2110 government off-the-shelf (GOTS) solutions to the acquirer. COTS solutions include non-
2111 developmental items (NDI), such as commercially licensing solutions/products, which include
2112 Open Source Solutions (OSS). GOTS solutions are government-only license-able solutions.
2113 Suppliers are a diverse group, ranging from very small to large, specialized to diversified, based
2114 in a single country to transnational, and range widely in the level of sophistication, resources,
2115 and transparency/visibility in both process and solution.
2116
2117 Suppliers also have diverse levels and types of C-SCRM practices in place. These practices and
2118 other related practices may provide the evidence needed for SCRM evaluation. An example of a
2119 federal resource that may be leveraged is the Defense Microelectronics Activity (DMEA)
2120 accreditation for Trusted Suppliers. When appropriate, allow suppliers the opportunity to reuse
2121 any existing data and documentation that may provide evidence of C-SCRM implementation.
2122
2123 Organizations should consider whether the cost of doing business with suppliers may be directly
2124 impacted by the extent of cyber supply chain requirements imposed on suppliers, the willingness
2125 or ability of suppliers to allow visibility into how their products are developed or manufactured
2126 and how they apply security and supply chain practices to their solutions. When organizations or
2127 system integrators require greater levels of transparency from suppliers, they must consider the
2128 possible cost implications of such requirements. Suppliers may opt not to participate in
2129 procurements to avoid increased costs or perceived risks to their intellectual property, limiting an
2130 organization’s supply or technology choices. Additionally, suppliers may face risk from
2131 customers imposing multiple, different sets of cyber supply chain requirements with which the
2132 supplier must comply on a per-customer basis.
2133

4.3.2 Developers

Developers are personnel that develop or manufacture systems, system components (e.g., software) or system services (e.g., Application Programming Interfaces (APIs)). Development can occur internally within organizations or through external entities. Developers typically maintain privileged access rights and play an essential role throughout the SDLC. The activities they perform and the work they produce can either enhance security or introduce new vulnerabilities. It is therefore essential that developers are both subject to, and intimately familiar with, C-SCRM requirements and controls.

4.3.3 System Integrators

System integrators are those entities which provide customized services to the acquirer including custom development, test, operations, and maintenance. This group usually replies to a request for proposal from an acquirer with a proposal describing a solution or service that is customized to the acquirer's requirements. Such proposals provided by system integrators can include many layers of suppliers and may include teaming arrangements with other vendors or subcontractors. The system integrator should ensure these business entities are vetted and verified with respect to the acquirer's C-SCRM requirements. Because of the level of visibility that can be obtained in the relationship with the system integrator, the acquirer has the discretion to require rigorous supplier acceptance criteria as well as any relevant countermeasures to address identified or potential risks.

4.3.4 External System Service Providers of Information System Services

Organizations use external service providers to perform or support some of their mission and business functions (NIST SP 800-53 Rev. 5). The outsourcing of systems and services creates a set of cyber supply chain concerns that reduces the acquirer's visibility into, and control of, the outsourced functions. Therefore, it requires increased rigor from organizations in defining C-SCRM requirements, stating them in procurement agreements, and then monitoring delivered services and evaluating them for compliance with the stated requirements. Regardless of who performs the services, the acquirer is ultimately responsible and accountable for the risk to the organization's systems and data that may result from using these services. Organizations should implement a set of compensating C-SCRM controls to address this risk and work with the mission/business process owner or risk executive to accept this risk. A variety of methods may be used to communicate and subsequently verify and monitor C-SCRM requirements through such vehicles as contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain transactions.

4.3.5 Other ICT/OT-related Service Providers

Providers of services can perform a wide range of different functions ranging from consulting to posting content on a website to janitorial services. Other ICT/OT-related Service Providers encompass those providers that require physical or logical access to ICT/OT or use technology (e.g., an aerial photographer using a drone to take video/pictures or a security firm remotely monitoring a facility using cloud-based video surveillance) as a means to deliver their service. As a result of service provider access or use, there is the potential for cyber-supply chain risk to be introduced to the organization.

Operational technology possesses unique operational and security characteristics that demand specialized skills and capabilities to effectively protect them. Organizations that have significant OT components throughout their enterprise architecture therefore often turn to specialized service providers for secure implementation and maintenance of these devices, systems, or equipment. Any organization or individual providing services which may include authorized access to an ICT or OT system should adhere to organizational C-SCRM requirements. Scrutiny should be paid particularly to ICT/OT-related service providers managing mission critical and/or safety-relevant assets.

4.4 SELECTING AND TAILORING IMPLEMENTING C-SCRM SECURITY CONTROLS

The C-SCRM controls defined in this section should be selected and tailored according to individual organization needs and environment using the guidance in NIST SP 800-53 Rev. 5, in order to ensure a cost-effective, risk-based approach to providing C-SCRM organization-wide. The C-SCRM baseline defined in this publication addresses the basic needs of a broad and diverse set of constituencies. Organizations must select, tailor, and implement the security controls based on: (i) the environments in which organizational information systems are acquired and operate; (ii) the nature of operations conducted by organizations; (iii) the types of threats facing organizations, missions/business processes, supply chains, and information systems; and (iv) the type of information processed, stored, or transmitted by information systems and the supply chain infrastructure.

After selecting the initial set of security controls, the acquirer should initiate the tailoring process according to NIST SP 800-53B *Control Baselines for Information Systems and Organization* in order to appropriately modify and more closely align the selected controls with the specific conditions within the organization. The tailoring should be coordinated with and approved by the appropriate organizational officials (e.g., authorizing officials, authorizing official designated representatives, risk executive (function), chief information officers, or senior information security officers) prior to implementing the C-SCRM controls. Additionally, organizations have the flexibility to perform the tailoring process at the enterprise level (either as the required tailored baseline or as the starting point for policy, program or system-specific tailoring), in support of a specific program at the individual information system level, or using a combination of enterprise-level, program/mission-level and system-specific approaches.

Selection and tailoring decisions, including the specific rationale for those decisions, should be included within the C-SCRM documentation at Levels 1, 2, and 3 and Appendix C and approved by the appropriate organizational officials as part of the C-SCRM Plan approval process.

4.4.1 C-SCRM Control Format

Table 4-2 shows the format used in this publication for controls which provide supplemental C-SCRM guidance on existing NIST SP 800-53 Rev. 5 controls or control enhancements.

C-SCRM controls that do not have a parent NIST SP 800-53 Rev. 5 control generally follow the format described in NIST SP 800-53 Rev. 5, with the addition of relevant levels. New controls

are given identifiers consistent with NIST SP 800-53 Rev. 5, but do not duplicate existing control identifiers.

Table 4-1: C-SCRM Control Format

CONTROL IDENTIFIER	CONTROL NAME
	Supplemental C-SCRM Guidance:
	Level(s):
	Related Control(s):
	Control Enhancement(s):
(1)	*CONTROL NAME | CONTROL ENHANCEMENT NAME*
	Supplemental C-SCRM Guidance:
	Level(s):
	Related Control(s):

An example of the C-SCRM control format is shown below using C-SCRM Control AC-3 and SCRM Control Enhancement AC-3(8):

AC-3 ACCESS ENFORCEMENT

Supplemental C-SCRM Guidance: Ensure that the information systems and the supply chain have appropriate access enforcement mechanisms in place. This includes both physical and logical access enforcement mechanisms, which likely work in coordination for supply chain needs. Organizations should ensure a detailed definition of access enforcement.

Level(s): 2, 3

Related Control(s): AC-4

Control Enhancement(s):

(8) ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS

(1) Supplemental C-SCRM Guidance: Prompt revocation is critical to ensure that suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers who no longer require access, or who abuse or violate their access privilege, are not able to access an organization's system. For example, in a "badge flipping" situation, a contract is transferred from one system integrator organization to another with the same personnel supporting the contract. In that situation, the organization should disable the existing accounts, retire the old credentials, establish new accounts, and issue completely new credentials.

Level(s): 2, 3

4.4.2 Using C-SCRM Controls in this Publication

The remainder of Section 4 provides the enhanced C-SCRM overlay of NIST SP 800-53 Rev. 5. This section displays the relationship between NIST SP 800-53 Revision 5 controls and C-SCRM controls in one of the following ways:

- If a NIST SP 800-53 Rev. 5 control or enhancement was determined to be an information security control that serves as a foundational control for C-SCRM, but is not specific to C-SCRM, it is not included in this publication.
- If a NIST SP 800-53 Rev. 5 control or enhancement was determined to be relevant to C-SCRM, the levels in which the control applies are also provided.
- If a NIST SP 800-53 Rev.5 enhancement was determined to be relevant to C-SCRM, but the parent control was not, the parent control number and title is included, but there is no supplemental C-SCRM guidance.
- C-SCRM controls/enhancements that do not have an associated NIST 800-53 Rev. 5 control/enhancement are listed with their titles and the control/enhancement text.
- All C-SCRM controls include the levels in which the control applies and supplemental C-SCRM guidance as applicable.
- When a control enhancement provides a mechanism for implementing the C-SCRM control, the control enhancement is listed within the Supplemental C-SCRM Guidance and is not included separately.
- If NIST SP 800-53 Rev. 5 already captures withdrawals or reorganization of prior NIST SP 800-161 controls, it is not included.

The following new controls and control enhancement have been added:

- The C-SCRM Control MA-8 – Maintenance Monitoring and Information Sharing is added to the Maintenance control family; and
- The C-SCRM Control SR-13 – Supplier Inventory is added to the Supply Chain Risk Management control family.

4.5 C-SCRM SECURITY CONTROLS

FAMILY: ACCESS CONTROL

FIPS 200 specifies the Access Control minimum security requirement as follows:

> *Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.*

Systems and components that traverse the supply chain are subject to access by a variety of individuals and organizations, including suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Such access should be defined and managed to ensure that it does not inadvertently result in unauthorized release, modification, or destruction of information. This access should be limited to only the necessary type, duration, and level of access for authorized organizations (and authorized individuals within those organizations) and monitored for cyber supply chain impact.

AC-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: Organizations should specify and include in agreements (e.g., contracting language) access control policies for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. These should include both physical and logical access to the cyber supply chain and the information system. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 1, 2, 3

AC-2 ACCOUNT MANAGEMENT

Supplemental C-SCRM Guidance: Use of this control helps establish traceability of actions and actors in the cyber supply chain. This control also helps ensure access authorizations of actors in the supply chain is appropriate on a continuous basis. The organization may choose to define a set of roles and associate a level of authorization to ensure proper implementation. Organizations must ensure that accounts for contractor personnel do not exceed the period of performance of the contract. Privileged accounts should only be established for appropriately vetted contractor personnel. Organizations should also have processes in place to establish and manage temporary or emergency accounts for contractor personnel that require access to a mission-critical or mission-enabling system during a continuity or emergency event. For example, during a pandemic event, existing contractor personnel who are not able to work due to illness may need to be temporarily backfilled by new contractor staff.

Level(s): 2, 3

AC-3 ACCESS ENFORCEMENT

Supplemental C-SCRM Guidance: Ensure that the information systems and the supply chain have appropriate access enforcement mechanisms in place. This includes both physical and logical access enforcement mechanisms, which likely work in coordination for supply chain needs. Organizations should ensure a defined consequence framework is in place to address access control violations.

Level(s): 2, 3

Control Enhancement(s):

(8) *ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS*

Supplemental C-SCRM Guidance: Prompt revocation is critical to ensure that suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers who no longer require access, or who abuse or violate their access privilege, are not able to access an organization's system. Organizations should include in their agreements a requirement for contractors, and sub-tier contractors, to immediately return access credentials (e.g., tokens, PIV or CAC cards, etc.) to the organization and organizations must have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrator organization to another with the same personnel supporting the contract. In that situation, the organization should disable the existing accounts, retire the old credentials, establish new accounts, and issue completely new credentials.

Level(s): 2, 3

(9) *ACCESS ENFORCEMENT | CONTROLLED RELEASE*

Supplemental C-SCRM Guidance: Information about the cyber supply chain should be controlled for release between the organization and third parties. Information may be exchanged between the organization and its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Controlled release of organizational information provides protection to manage risks associated with disclosure.

Level(s): 2, 3

AC-4 INFORMATION FLOW ENFORCEMENT

Supplemental C- SCRM Guidance: Supply chain information may traverse a large cyber supply chain to a broad set of stakeholders including the organization and its various federal stakeholders, as well as suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Specifying the requirements as well as how information flow is enforced should ensure that only the required information, and not more, is communicated to the various participants in the cyber supply chain. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2, 3

Control Enhancement(s):

(6) *INFORMATION FLOW ENFORCEMENT | METADATA*

Supplemental C-SCRM Guidance: Metadata relevant to C-SCRM is quite extensive and includes activities within the SDLC. For example, information about systems and system components, acquisition details, and delivery is considered metadata and may require appropriate protections. Organizations should identify what metadata is directly relevant to their supply chain security and ensure that information flow enforcement is implemented in order to protect applicable metadata.

Level(s): 2, 3

(17) *INFORMATION FLOW ENFORCEMENT | DOMAIN AUTHENTICATION*

Supplemental C-SCRM Guidance: Within the C-SCRM context, organizations should specify various source and destination points for information about the cyber supply chain and information that flows through the cyber supply chain. This is so that organizations have visibility of information flow within the cyber supply chain.

Level(s): 2, 3

(19) *INFORMATION FLOW ENFORCEMENT | VALIDATION OF METADATA*

Supplemental C-SCRM Guidance: For C-SCRM, validation of data and the relationship to its metadata are critical. Much of the data transmitted through the cyber supply chain is validated with the verification of the associated metadata that is bound to it. Ensure that proper filtering and inspection is put in place for validation before allowing payloads into the cyber supply chain.

Level(s): 2, 3

(21) *INFORMATION FLOW ENFORCEMENT | PHYSICAL OR LOGICAL SEPARATION OF INFORMATION FLOWS*

Supplemental C-SCRM Guidance: The organization should ensure the separation of the information system and cyber supply chain information flow. Various mechanisms can be implemented including, for example, encryption methods (e.g., digital signing). Addressing information flow between the organization and its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers may be challenging, especially when leveraging public networks.

Level(s): 3

AC-5 SEPARATION OF DUTIES

Supplemental C-SCRM Guidance: The organization should ensure that appropriate separation of duties is established for decisions requiring the acquisition of both information system and cyber supply chain components. Separation of duties helps to ensure that adequate protections are in place for components entering the organization's cyber supply chain. An example may be developers not having privileges to promote code they wrote from development to production environments.

Level(s): 2, 3

AC-6 LEAST PRIVILEGE

Supplemental C-SCRM Guidance: For C-SCRM supplemental guidance, see control enhancements.

Control Enhancement(s):

(6) *LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS*

Supplemental C-SCRM Guidance: Organizations should ensure that protections are in place to prevent non-organizational users from having privileged access to organizational cyber supply chain and related supply chain information. When organizational users may include independent consultants, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, relevant access requirements may need to be more precisely defined regarding which information and/or components are accessible, for what duration, at which frequency, using which access methods, and by whom, using least privilege mechanisms. Understanding which components are critical and noncritical can aid in understanding the level of detail that may need to be defined regarding least privilege access for non-organizational users.

Level(s): 2, 3

AC-17 REMOTE ACCESS

Supplemental C-SCRM Guidance: Evermore frequently, cyber supply chains are accessed remotely. Whether for the purpose of development, maintenance, or operation of information systems, organizations should implement secure remote access mechanisms and allow remote access only to vetted personnel. Remote access to an organization's cyber supply chain (including distributed software development environments) should be limited to the organization or contractor personnel and only if and as required to perform their tasks. Remote access requirements, such as a requirement to use a secure VPN, employ multi-factor authentication, limit access to specified business hours, or from specified geographic locations, must be properly defined in agreements. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2, 3

Control Enhancement(s):

(6) *REMOTE ACCESS | PROTECTION OF MECHANISM INFORMATION*

Supplemental C-SCRM Guidance: Organizations should ensure that detailed requirements are properly defined and access to information regarding the information system and cyber supply chain is protected from unauthorized use and disclosure. Since cyber supply chain data and metadata disclosure or access can have significant implications to an organization's mission processes, appropriate measures must be taken to vet both the cyber supply chain and personnel processes to ensure that adequate protections are implemented. Ensure that remote access to such information is included in requirements.

Level(s): 2, 3

AC-18 WIRELESS ACCESS

Supplemental C-SCRM Guidance: An organization's cyber supply chain may include wireless infrastructure that supports supply chain logistics (e.g., Radio Frequency Identification Device (RFID) support, software call home features). Supply chain systems/components traverse the cyber supply chain as they are moved from one location to another, whether within the organization's own environment or during delivery from system integrators or suppliers. Ensuring appropriate access mechanisms are in place within this cyber supply chain enables the protection of the information systems and components, as well as logistics technologies and metadata used during shipping (e.g., within tracking sensors). The organization should explicitly define appropriate wireless access control mechanisms for the cyber supply chain in policy and implement appropriate mechanisms.

Level(s): 1, 2, 3

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Supplemental C-SCRM Guidance: Use of mobile devices (e.g., laptops, tablets, e-readers, smartphones, smartwatches) has become common in the cyber supply chain. They are used in direct support of an organization's operations as well as for purposes such as tracking supply chain logistics data as information systems and components traverse organization or systems integrator supply chains. Ensure that access control mechanisms are clearly defined and implemented where relevant when managing organizations cyber supply chain components. An example of such an implementation includes access control mechanisms implemented for use with remote handheld units in RFID for tracking components that

traverse the supply chain. Access control mechanisms should also be implemented on any associated data and metadata tied to the devices.

Level(s): 2, 3

AC-20 USE OF EXTERNAL SYSTEMS

Supplemental C-SCRM Guidance: Organizations' external information systems include those of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Unlike in an acquirer's internal organization where direct and continuous monitoring is possible, in the external supplier relationship, information may be shared on an as-needed basis and should be articulated in an agreement. Access to the cyber supply chain from such external information systems should be monitored and audited. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 1, 2, 3

Control Enhancement(s):

(1) *USE OF EXTERNAL SYSTEMS | LIMITS ON AUTHORIZED USE*

Supplemental C-SCRM Guidance: This enhancement helps limit exposure of the cyber supply chain to the suppliers', developers', system integrators', external system service providers', and other ICT/OT-related service providers' systems.

Level(s): 2, 3

(3) *USE OF EXTERNAL SYSTEMS | NON-ORGANIZATIONALLY OWNED SYSTEMS — RESTRICTED USE*

Supplemental C-SCRM Guidance: Devices that do not belong to the organization (e.g., bring your own device (BYOD) policies) increase the organization's exposure to cyber supply chain risks. This includes devices used by suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Organizations should review the use of non-organization devices by non-organization personnel and make a risk-based decision as to whether it will allow use of such devices or furnish devices. Organizations should furnish devices to those non-organization personnel that present unacceptable cyber supply chain risk.

Level(s): 2, 3

AC-21 INFORMATION SHARING

Supplemental C-SCRM Guidance: Sharing information within the cyber supply chain can help to manage cyber supply chain risks. This information may include vulnerabilities, threats, criticality of systems and components, or delivery information. This information sharing should be carefully managed to ensure that the information is accessible only to authorized individuals within the organization's cyber supply chain. Organizations should clearly define boundaries for information sharing with respect to temporal, informational, contractual, security, access, system, and other requirements. Organizations should monitor and review for unintentional or intentional information sharing within its cyber supply chain activities including information sharing with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

Level(s): 1, 2

AC-22 PUBLICLY ACCESSIBLE CONTENT

Supplemental C-SCRM Guidance: Within the C-SCRM context, publicly accessible content may include Requests for Information, Requests for Proposal, or information about delivery of systems and components. This information should be reviewed to ensure that only appropriate content is released for public consumption, alone or in aggregation with other information.

Level(s): 2, 3

AC-23 DATA MINING PROTECTION

Supplemental C-SCRM Guidance: Organizations should require its prime contractors to implement this control as part of their insider threat activities and flow down this requirement to relevant sub-tier contractors.

Level(s): 2, 3

AC-24 ACCESS CONTROL DECISIONS

Supplemental C-SCRM Guidance: Organizations should assign access control decisions to support authorized accesses to the cyber supply chain. Ensure that if a system integrator or external service provider is used, there is consistency in access control decision requirements and how the requirements are implemented to deliver consistency in support of the organization's supply chain needs. This may require defining such requirements in service-level agreements in many cases as part of the upfront relationship established between the organization and system integrator or the organization and external service provider. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 1, 2, 3

FAMILY: AWARENESS AND TRAINING

FIPS 200 specifies the Awareness and Training minimum security requirement as follows:

> *Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.*

NIST SP 800-161 Rev. 1 expands the Awareness and Training control of FIPS 200 to include C-SCRM. Making the workforce aware of C-SCRM concerns is key to a successful C-SCRM strategy. C-SCRM awareness and training provides understanding of the problem space and of the appropriate processes and controls that can help mitigate cyber supply chain risk. Organizations should provide C-SCRM awareness and training to individuals at all levels within the organization including, for example, information security, procurement, enterprise risk management, engineering, software development, IT, legal, HR, and others. Organizations should also work with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to ensure the personnel that interact with an organization's cyber supply chains receive C-SCRM awareness and training, as appropriate.

AT-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: Organizations should designate a specific official to manage the development, documentation, and dissemination of the awareness and training policy and procedures that includes C-SCRM as well as role-based specific training for those with supply chain responsibilities. Organizations should integrate cyber supply chain risk management training and awareness into the security training and awareness policy. The C-SCRM training should target both the organization and its contractors. The policy should ensure that cyber supply chain role-based training is required for those individuals or functions that touch or impact the cyber supply chain, such as information system owner, acquisition, supply chain logistics, system engineering, program management, IT, quality, and incident response.

C-SCRM training procedures should address:

a. Roles throughout the cyber supply chain and system/element life cycle to limit opportunities and means available to individuals performing these roles that could result in adverse consequences;
b. Requirements for interaction between an organization's personnel and individuals not employed by the organization that participate in the cyber supply chain throughout the SDLC; and
c. Incorporating feedback and lessons learned from C-SCRM activities into the C-SCRM training.

Level(s): 1, 2

AT-2 LITERACY TRAINING AND AWARENESS

Supplemental C-SCRM Guidance: C-SCRM-specific supplemental guidance provided in control enhancements.

Control Enhancements:

(1) *LITERACY TRAINING AND AWARENESS | PRACTICAL EXERCISES*

Supplemental C-SCRM Guidance: Organizations should provide practical exercises in literacy training that simulate cyber supply chain events and incidents. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-level contractors

(2) *LITERACY TRAINING AND AWARENESS | INSIDER THREAT*

Supplemental C-SCRM Guidance: Organizations should provide literacy training on recognizing and reporting potential indicators of insider threat within the cyber supply chain. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

(3) *LITERACY TRAINING AND AWARENESS | SOCIAL ENGINEERING AND MINING*

Supplemental C-SCRM Guidance: Organizations should provide literacy training on recognizing and reporting potential and actual instance of cyber supply chain related social engineering and social mining. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-level contractors

(4) *LITERACY TRAINING AND AWARENESS | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR*

Supplemental C-SCRM Guidance: Provide literacy training on recognizing suspicious communications on anomalous behavior in organizational supply chain systems. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-level contractors.

(5) *LITERACY TRAINING AND AWARENESS | ADVANCED PERSISTENT THREAT*

Supplemental C-SCRM Guidance: Provide literacy training on recognizing suspicious communications on advanced persistent threat (APT) in the organization's cyber supply chain. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-level contractors

(6) *LITERACY TRAINING AND AWARENESS | CYBER THREAT ENVIRONMENT*

Supplemental C-SCRM Guidance: Provide literacy training on cyber threats specific to the organization's supply chain environment. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-level contractors

Level(s): 2

AT-3 ROLE-BASED TRAINING

Supplemental C-SCRM Guidance: Addressing cyber-supply chain risks throughout the acquisition process is essential to performing C-SCRM effectively. Personnel who are part of the acquisition workforce require training on what C-SCRM requirements, clauses, and evaluation factors are necessary to include when conducting a procurement and how to incorporate C-SCRM into each acquisition phase. Similar enhanced training requirements should be tailored for personnel responsible for conducting threat assessments and involved in responding to threats and identified risks require training in counter-intelligence awareness and reporting.

Control Enhancement(s):

(7) *SECURITY TRAINING | PHYSICAL SECURITY CONTROLS*

Supplemental C-SCRM Guidance: C-SCRM is impacted by a number of physical security mechanisms and procedures within the supply chain, such as manufacturing, shipping, and receiving, physical access to facilities, inventory management, and warehousing. Organization and system integrator personnel providing development and operational support to the organization should receive training on how to handle these physical security mechanisms and on the associated cyber supply chain risks.

Level(s): 2

(6) *ROLE-BASED TRAINING | COUNTERINTELLIGENCE TRAINING*

Supplemental C-SCRM Guidance: Public sector organizations should provide specialized counterintelligence awareness training that enables its resources to collect, interpret, and act upon a range of data sources that may signal the presence of a foreign adversary's presence in the cyber supply chain. Counterintelligence training should at a minimum cover known red flags, key information sharing concepts, and reporting requirements.

Level(s): 2

AT-4 TRAINING RECORDS

Supplemental C-SCRM Guidance: Organizations should maintain documentation for C-SCRM-specific training, especially in regard to key personnel in acquisitions and counterintelligence.

Level(s): 2

FAMILY: AUDIT AND ACCOUNTABILITY

FIPS 200 specifies the Audit and Accountability minimum security requirement as follows:

> *Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.*

Audit and accountability controls for C-SCRM provide information useful in the event of a cyber supply chain incident or compromise. Organizations should ensure they designate and audit cyber supply chain-relevant events within their information system boundaries using appropriate audit mechanisms (e.g., system logs, Intrusion Detection System (IDS) logs, firewall logs, paper reports, forms, clipboard checklists, digital records). These audit mechanisms should also be configured to work within reasonable time-frame boundaries, as defined by organizational policy. Organizations may encourage their system suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to do the same and may include in agreements requirements for such monitoring. However, organizations should not deploy audit mechanisms on systems outside of their organizational boundary, including those of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

AU-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: Organizations must designate a specific official to manage the development, documentation, and dissemination of the audit and accountability policy and procedures to include auditing of the supply chain information systems and network. Audit mechanisms provide data for tracking activities in an organization's supply chain information systems and network. Audit and accountability policy and procedures should appropriately address such tracking and its availability for other various supply chain activities, such as configuration management. Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers activities should not be included in such policy, unless those are performed within the acquirer's supply chain information systems and network. Audit and accountability policy procedures should appropriately address supplier audits as a way to examine the quality of a particular supplier and the risk it presents to the organization and the organization's supply chain.

Level(s): 1, 2, 3

AU-2 EVENT LOGGING

Supplemental C-SCRM Guidance: An observable occurrence within the information system or supply chain network should be identified as a supply chain auditable event, based on the organization's SDLC context and requirements. Auditable events may include software/hardware changes, failed attempts to access supply chain information systems, or movement of source code. Information on such events should be captured by appropriate audit mechanisms and should be traceable and verifiable. Information captured may include type of event, date/time, length, and frequency of occurrence. Among other things, auditing may help detect misuse of the supply chain information systems or network caused by insider threat. Logs are a key resource when identifying operational trends and long-term problems, and as such organizations should incorporate reviewing logs at contract renewal point for vendors to determine whether there is systemic problem.

Level(s): 1, 2, 3

AU-3 CONTENT OF AUDIT RECORDS

Supplemental C-SCRM Guidance: Audit records of a supply chain event should be handled and maintained in a manner that conforms to record retention requirements, preserves the integrity of the findings, and as appropriate, the confidentiality of the record information and its source(s). In certain instances, such records may be used in administrative or legal proceedings.

Level(s): 1, 2, 3

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

Supplemental C-SCRM Guidance: The organization should ensure that both supply chain and information security auditable events are appropriately filtered and correlated for analysis and reporting. For example, if new maintenance or a patch upgrade is recognized to have an invalid digital signature, the identification of the patch arrival qualifies as a supply chain auditable event, while invalid signature is an information security auditable event. The combination of these two events may provide information valuable to C-SCRM. The organization should adjust the level of audit record review based on risk changes (e.g., active threat intel, risk profile) on a specific vendor. Contracts should explicitly address how audit findings will be reported and adjudicated.

Level(s): 2, 3

Control Enhancement(s):

(9) *AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES*

Supplemental C-SCRM Guidance: In a C-SCRM context, nontechnical sources include changes to organizational security or operational policy, changes to procurement or contracting processes, and notifications from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers regarding plans to update, enhance, patch, or retire/dispose of a system/component.

Level(s): 3

AU-10 NON-REPUDIATION

Supplemental C-SCRM Guidance: Organizations should implement non-repudiation techniques to protect both information systems and supply chain network. Examples of what may require non-repudiation include supply chain metadata describing the components, supply chain communication, delivery acceptance information, etc. For information systems, it can be patch or maintenance upgrades for software as well as component replacement in a large hardware system. Verifying that such components originate from the OEM is part of non-repudiation.

Level(s): 3

Control Enhancement(s):

(1) *NON-REPUDIATION | ASSOCIATION OF IDENTITIES*

Supplemental C-SCRM Guidance: This enhancement helps traceability in cyber supply chain. It also facilitates the accuracy of provenance.

Level(s): 2

(2) *NON-REPUDIATION | VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY*

Supplemental C-SCRM Guidance: This enhancement validates the relationship of provenance and a component within the supply chain. Therefore, it ensures integrity of provenance.

Level(s): 2, 3

(3) *NON-REPUDIATION | CHAIN OF CUSTODY*

Supplemental C-SCRM Guidance: Chain of custody is fundamental to provenance and traceability in the cyber supply chain. It also helps verification of system and component integrity.

Level(s): 2, 3

AU-12 AUDIT RECORD GENERATION

Supplemental C-SCRM Guidance: Organizations should ensure that audit record generation mechanisms are in place to capture all relevant supply chain auditable events. Examples of such events include: component version updates, component approvals from acceptance testing results, logistics data-capturing inventory, or transportation information.

Level(s): 2, 3

AU-13 MONITORING FOR INFORMATION DISCLOSURE

Supplemental C-SCRM Guidance: Within the C-SCRM context, information disclosure may occur via multiple avenues including open source information. For example, supplier-provided errata may reveal information about an organization's system that may provide insight into the system that increases the risk to the system. Organizations should ensure monitoring is in place for contractor systems to detect unauthorized disclosure of any data and ensure contract language includes a requirement that the vendor will notify the organization, in accordance with organizationally-defined timeframes and as soon as possible in the event of any potential or actual unauthorized disclosure.

Level(s): 2, 3

AU-14 SESSION AUDIT

Supplemental C-SCRM Guidance: Organizations should include non-federal contract employees in session audits to identify security risks in the supply chain.

Level(s): 2, 3

AU-16 CROSS-ORGANIZATIONAL AUDIT LOGGING

Supplemental C-SCRM Guidance: In a C-SCRM context, this control includes the organization's use of system integrator or external service provider infrastructure. Organizations should add language to contracts on coordinating audit information requirements and information exchange agreements with vendors.

Level(s): 2, 3

Control Enhancement(s):

(2) *CROSS-ORGANIZATIONAL AUDIT LOGGING | SHARING OF AUDIT INFORMATION*

Supplemental C-SCRM Guidance: Whether managing a distributed audit environment or an audit data-sharing environment between organizations and its system integrators or external services providers, organizations should establish a set of requirements for the process of sharing audit information. In the case of the system integrator and external service provider and the organization, a service-level agreement of the type of audit data required vs. what can be provided must be agreed to in advance to ensure that the organization obtains the relevant audit information needed for ensuring that appropriate protections are in place to meet its mission operation protection needs. Ensure that coverage of both information systems and supply chain network are addressed for the collection and sharing of audit information. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-level contractors.

Level(s): 2, 3

FAMILY: ASSESSMENT, AUTHORIZATION, AND MONITORING

FIPS 200 specifies the Certification, Accreditation, and Security Assessments minimum security requirement as follows:

> *Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.*

Organizations should integrate C-SCRM, including the supply chain risk management process and the use of relevant controls defined in this publication, into ongoing security assessment and authorization activities. This includes activities to assess and authorize an organization's information systems, as well as external assessments of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, where appropriate. Cyber supply chain aspects include documentation and tracking of chain of custody and system interconnections within and between organizations, verification cyber supply chain security training, verification of suppliers claims of conformance to security, product/component integrity, and validation tools and techniques for noninvasive approaches to detecting counterfeits or malware (e.g., Trojans) using inspection for genuine components including manual inspection techniques.

CA-1 POLICY AND PROCEDURES

Supplemental C- SCRM Guidance: Integrate the development and implementation of assessment and authorization policies and procedures for cyber supply chain security into the control assessment and authorization policy, and related C-SCRM Strategy/Implementation Plan(s), policies, and system-level plans. To address cyber supply chain risks, organizations should develop a C-SCRM policy (or, if required, integrate into existing policies) to direct C-SCRM activities for control assessment and authorization. The C-SCRM policy should define C-SCRM roles and responsibilities within the organization for conducting control assessment and authorization, any dependencies among those roles, and the interaction among the roles. Organization-wide security and privacy risk should be assessed on an ongoing basis and include supply chain risk assessment results.

Level(s): 1, 2, 3

CA-2 CONTROL ASSESSMENTS

Supplemental C-SCRM Guidance: Ensure that the control assessment plan incorporates relevant C-SCRM controls and control enhancements. The control assessment should cover the assessment of both information systems and the supply chain and ensure that an organization-relevant baseline set of controls and control enhancements are identified and used for the assessment. Control assessments can include information from supplier audits, reviews, and supply chain-related information. Organizations should develop a strategy for collecting information, including a strategy for engaging with providers on supply chain risk assessments. Such collaboration helps organizations leverage information from providers, reduce

redundancy, identify potential courses of action for risk responses, and reduce the burden on providers. C-SCRM personnel should review the control assessment.

Level(s): 2, 3

Control Enhancement(s):

(2) *CONTROL ASSESSMENTS | SPECIALIZED ASSESSMENTS*

Supplemental C-SCRM Guidance: Organizations should use a variety of assessment techniques and methodologies such as continuous monitoring, insider threat assessment, and malicious user's assessment. These assessment mechanisms are context-specific and require the organization to understand its supply chain and to define the required set of measures for assessing and verifying that appropriate protections have been implemented.

Level(s): 3

(3) *CONTROL ASSESSMENTS | LEVERAGING RESULTS FROM EXTERNAL ORGANIZATIONS*

Supplemental C-SCRM Guidance: For C-SCRM, organizations should use external security assessments for suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. External assessments include certifications, third-party assessments, and, in the federal context, prior assessments performed by other departments and agencies. Organizations such as the International Organization for Standardization (ISO), the National Information Assurance Partnership (Common Criteria), and the Open Group Trusted Technology Forum (OTTF) certifications may also be used by non-federal and federal organizations alike, if such certifications meet agency needs.

Level(s): 3

CA-3 INFORMATION EXCHANGE

Supplemental C-SCRM Guidance: Exchange of information or data between the system and other systems require scrutiny from a supply chain perspective. This includes understanding the interface characteristics and connections of those components/systems that are directly interconnected to or the data that is shared through those components/systems with developers, system integrators, external system service providers, other ICT/OT-related service providers and, in some cases, suppliers. Ensure that proper service-level agreements are in place to ensure compliance to system information exchange requirements defined by the organization, as the transfer of information between systems in different security or privacy domains with different security or privacy policies introduces risk that such transfers violate one or more domain security or privacy policies. Examples of such interconnections can include:

a. A shared development and operational environment between the organization and system integrator;
b. Product update/patch management connection to an off-the-shelf supplier; and
c. Data request and retrieval transactions in a processing system residing on an external service provider shared environment.

Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 3

CA-5 PLAN OF ACTION AND MILESTONES

Supplemental C-SCRM Guidance: For system-level plan of actions and milestones (POA&Ms), organizations need to ensure that a separate POA&M exists for C-SCRM include both information systems and the supply chain. The C-SCRM POA&M should include tasks to be accomplished with a recommendation for completion before or after system authorization; resources required to accomplish the tasks; milestones established to meet the tasks; and the scheduled completion dates for the milestones and tasks. The organization should include in its C-SCRM POA&M relevant weaknesses, impact of weaknesses on information systems or the supply chain, any remediation to address weaknesses, and any continuous monitoring activities. The C-SCRM POA&M should be included as part of the authorization package.

Level(s): 2, 3

CA-6 AUTHORIZATION

Supplemental C-SCRM Guidance: Authorizing officials should include C-SCRM in authorization decisions. To accomplish this, supply chain risks and compensating controls documented in C-SCRM Plans or system security plans, and C-SCRM plan of action and milestones should be included in the authorization package as part of the decision-making process. Risks should be determined and associated compensating controls selected based on output from criticality, threat, and vulnerability analyses. Authorizing officials may use guidance in Section 2 of this document as well as NISTIR 8179 to guide the assessment process.

Level(s): 1, 2, 3

CA-7 CONTINUOUS MONITORING

Supplemental C-SCRM Guidance: For C-SCRM-specific guidance on this control, see Section 2 of this publication.

Level(s): 1, 2, 3

Control Enhancement(s):

(3) *CONTINUOUS MONITORING | TREND ANALYSES*

Supplemental C-SCRM Guidance: Information gathered during continuous monitoring/trend analysis serves as input into C-SCRM decisions including criticality analysis, vulnerability and threat analysis, and risk assessment. It also provides information that can be used in incident response and potentially can identify a cyber supply chain compromise, including insider threat.

Level(s): 3

FAMILY: CONFIGURATION MANAGEMENT

FIPS 200 specifies the Configuration Management minimum security requirement as follows:

> *Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.*

Configuration Management helps track systems, components, and documentation within the information systems, networks, and throughout the SDLC. This is important for knowing what changes were made to those systems, components, and documentation, who made the changes, and who authorized the changes. Fundamentally, configuration management provides tools to establish the chain of custody for systems, components, and documentation. Configuration management also provides evidence for investigations of cyber supply chain compromise when determining which changes were authorized and which were not, and therefore provides useful information. Organizations should apply configuration management controls to their own systems and encourage use of configuration management controls by their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. See NISTIR 7622 for more information on Configuration Management.

CM-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: Configuration management impacts nearly every aspect of the cyber supply chain. Configuration Management is critical for organization's ability to establish provenance of components to include tracking and tracing them through the SDLC and through the supply chain. Properly defined and implemented configuration management capability provides greater assurance throughout the SDLC and the supply chain that components are authentic and have not been inappropriately modified. When defining configuration management policy and procedures, organizations should address the full SDLC. This should include procedures for introducing and removing components to and from the organization's information system boundary. Configuration Management policy should incorporate configuration items, data retention for configuration items and corresponding metadata, and tracking of the configuration item and its metadata. The organization should coordinate with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers regarding the configuration management policy.

Level(s): 1, 2, 3

CM-2 BASELINE CONFIGURATION

Supplemental C-SCRM Guidance: Organizations should establish a baseline configuration of both the information system and the development environment including documenting, formally reviewing, and securing the agreement of stakeholders. The purpose of the baseline is to provide a starting point for tracking the changes to components, code, and/or settings throughout the SDLC. Regular reviews and updates of baseline configurations (i.e., re-baselining) are critical for traceability and provenance. The baseline configuration must take into consideration the organization's operational environment and any relevant suppliers', developers', system integrators', external system service providers', and other ICT/OT-related service providers' involvement within the organization's information systems and networks. If the

system integrator, for example, uses the existing organization's infrastructure, appropriate measures should be taken to establish a baseline that reflects an appropriate set of agreed-upon criteria for access and operation.

Level(s): 2, 3

Control Enhancement(s):

(6) *BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS*

Supplemental C-SCRM Guidance: The organization should maintain or require the maintenance of a baseline configuration of applicable suppliers', developers', system integrators', external system service providers', and other ICT/OT-related service providers' development, test (and if applicable, staging) environments as well as any configuration of interfaces.

Level(s): 2, 3

CM-3 CONFIGURATION CHANGE CONTROL

Supplemental C-SCRM Guidance: Organizations should determine, implement, monitor, and audit configuration settings and change controls within the information systems and networks and throughout the SDLC. This control supports traceability for C-SCRM. The below NIST SP 800-53 Rev. 5 control enhancements CM-3 (1), (2), (4), and (8) are mechanisms that can be used for C-SCRM to collect and manage change control data.

Level(s): 2, 3

(1) *CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENTATION, NOTIFICATION, AND PROHIBITION OF CHANGES*

Supplemental C-SCRM Guidance: Organizations should define a set of system changes that are critical to the protection of the information system and the underlying or interoperating systems and networks. These changes may be defined based on a criticality analysis (including components, processes, and functions) and where vulnerabilities exist that are not yet remediated (e.g., due to resource constraints). The change control process should also monitor for changes that may affect an existing security control to ensure that this control continues to function as required.

Level(s): 2, 3

(2) *CONFIGURATION CHANGE CONTROL | TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES*

Supplemental C-SCRM Guidance: Test, validate, and document changes to the system before finalizing the implementation of the changes.

Level(s): 2, 3

(4) *CONFIGURATION CHANGE CONTROL | SECURITY AND PRIVACY REPRESENTATIVES*

Supplemental C-SCRM Guidance: Require organization security and privacy representatives] to be members of the configuration change control function.

Level(s): 2, 3

(8) *CONFIGURATION CHANGE CONTROL | PREVENT OR RESTRICT CONFIGURATION CHANGES*

Supplemental C-SCRM Guidance: Prevent or restrict changes to the configuration of the system under organization-defined circumstances.

Level(s): 2, 3

CM-4 IMPACT ANALYSIS

Supplemental C-SCRM Guidance: Organizations should take under consideration changes to the information system and underlying or interoperable systems and networks to determine whether the impact of these changes affects existing security control(s) and warrants additional or different protection to maintain an acceptable level of cyber supply chain risk. Ensure that stakeholders, such as system engineers and system security engineers are included in the impact analysis activities to provide their perspectives for C-SCRM. NIST SP 800-53 Rev. 5 control enhancement CM-4 (1) is a mechanism that can be used to protect the information system and from vulnerabilities that may be introduced through the test environment.

Level(s): 3

(1) *IMPACT ANALYSES | SEPARATE TEST ENVIRONMENTS*

Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice

Level(s): 3

Related Control(s): SA-11, SC-7

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Supplemental C-SCRM Guidance: Organizations should ensure that requirements regarding physical and logical access restrictions for changes to the information systems and networks are defined and included in the organization's implementation of access restrictions. Examples include access restriction for changes to centrally managed processes for software component updates and the deployment of updates or patches.

Level(s): 2, 3

Control Enhancements:

(1) *ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT AND AUDIT RECORDS*

Supplemental C-SCRM Guidance: Organizations should implement mechanisms to ensure automated access enforcement and auditing of the information system and the underlying systems and networks.

Level(s): 3

(6) *ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES*

Supplemental C-SCRM Guidance: Organizations should note that software libraries may be considered configuration items, access to which should be managed and controlled.

Level(s): 3

CM-6 CONFIGURATION SETTINGS

Supplemental C-SCRM Guidance: Organizations should oversee the function of modifying configuration settings for their information systems and networks and throughout the SDLC. Methods of oversight include periodic verification, reporting, and review. Resulting information may be shared with various parties that have access to, are connected to, or engage in creation of the organization's information systems and networks on a need-to-know basis. Changes should be tested and approved before they are implemented. Configuration settings should be monitored and audited to alert designated organizational personnel when a change has occurred.

Level(s): 2, 3

Control Enhancement(s):

(1) *CONFIGURATION SETTINGS | AUTOMATED MANAGEMENT, APPLICATION, AND VERIFICATION*

Supplemental C-SCRM Guidance: The organization should, when feasible, employ automated mechanisms to manage, apply, and verify configuration settings.

Level(s): 3

(2) *CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES*

Supplemental C-SCRM Guidance: The organization should ensure that designated security or IT personnel are alerted regarding unauthorized changes to configuration settings. When suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers are responsible for such unauthorized changes, this qualifies as a C-SCRM incident that should be recorded and tracked to monitor trends. For a more comprehensive view, a specific, predefined set of C-SCRM stakeholders should assess the cyber supply chain risk impact of unauthorized changes in the supply chain. When impact is assessed, relevant stakeholders should help define and implement appropriate mitigation strategies to ensure a comprehensive resolution.

Level(s): 3

CM-7 LEAST FUNCTIONALITY

Supplemental C-SCRM Guidance: Least functionality reduces the attack surface of cyber supply chain risks. Organizations should select components that allow the flexibility and option for specifying and implementing least functionality. Organizations should ensure least functionality in their information systems and networks and throughout SDLC. NIST SP 800-53 Rev. 5 control enhancement CM-7 (9) mechanism can be used to protect information systems and networks from vulnerabilities that may be introduced by the use of unauthorized hardware being connected to organizational systems.

Level(s): 3

Control Enhancement(s):

(1) *LEAST FUNCTIONALITY | PERIODIC REVIEW*

Supplemental C-SCRM Guidance: Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2, 3

(4) *LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE*

Supplemental C-SCRM Guidance: Organizations should define requirements and deploy appropriate processes to specify and detect software that is not allowed. This can be aided by defining a

requirement to, at a minimum, not use disreputable or unauthorized software. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2, 3

(5) *LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE*

Supplemental C-SCRM Guidance: Organizations should define requirements and deploy appropriate processes to specify allowable software. This can be aided by defining a requirement to use only reputable software. This can include requirements for alerts when new software and updates to software are introduced into the organization's environment. An example of such requirements is to allow open source software only if the code is available for an organization's evaluation and determined to be acceptable for use.

Level(s): 3

(6) *LEAST FUNCTIONALITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES*

Supplemental C-SCRM Guidance: The organization should ensure that code authentication mechanisms such as digital signatures are implemented when executing code to assure the integrity of software, firmware, and information of the information systems and networks.

Level(s): 2, 3

(7) *LEAST FUNCTIONALITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS*

Supplemental C-SCRM Guidance: The organization should obtain binary or machine-executable code directly from the OEM/developer or other acceptable, verified source.

Level(s): 3

(8) *LEAST FUNCTIONALITY | BINARY OR MACHINE EXECUTABLE CODE*

Supplemental C-SCRM Guidance: When exceptions are made to use software products without accompanying source code or from sources with limited or no warranty because of compelling mission or operational requirements, approval by the authorizing official should be contingent upon the organization explicitly incorporating cyber supply chain risks in the assessment of such software products and the implementation of compensating controls to address any identified and assessed risks.

Level(s): 2, 3

(9) *LEAST FUNCTIONALITY | PROHIBITING THE USE OF UNAUTHORIZED HARDWARE*

Organizations should define requirements and deploy appropriate processes to specify and detect hardware that is not allowed. This can be aided by defining a requirement to, at a minimum, not use disreputable or unauthorized hardware. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors

Level(s): 2, 3

CM-8 SYSTEM COMPONENT INVENTORY

Supplemental C-SCRM Guidance: Organizations should ensure that critical component assets within the information systems and networks are included in the asset inventory. The inventory must include information for critical component accountability. Inventory information includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.

Level(s): 2, 3

Control Enhancement(s):

(1) *SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATION AND REMOVAL*

Supplemental C-SCRM Guidance: When installing, updating, or removing an information system, information system component, or network component, the organization needs to update the inventory to ensure traceability for tracking critical components. In addition, the information system's configuration needs to be updated to ensure an accurate inventory of supply chain protections, and re-baselined accordingly.

Level(s): 3

(2) *SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE*

Supplemental C-SCRM Guidance: The organization should implement automated maintenance mechanisms to ensure that changes to component inventory for the information systems and networks are monitored for installation, update, and removal. When automated maintenance is performed with a predefined frequency and with the automated collation of relevant inventory information about each defined component, the organization should ensure that updates are available to relevant stakeholders for evaluation. Predefined frequencies for data collection should be less predictable in order to reduce the risk of an insider threat bypassing security mechanisms.

Level(s): 3

(4) *SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION*

Supplemental C-SCRM Guidance: The organization should ensure that accountability information is collected for information system and network components. The system/component inventory information should identify those individuals who originate an acquisition as well as intended end users, including any associated personnel who may administer or use the system/components.

Level(s): 3

(6) *SYSTEM COMPONENT INVENTORY | ASSESSED CONFIGURATIONS AND APPROVED DEVIATIONS*

Supplemental C-SCRM Guidance: Assessed configurations and approved deviations must be documented and tracked. Any changes to the baseline configurations of information systems and networks require a review by relevant stakeholders to ensure that the changes do not result in increased cyber supply chain risk.

Level(s): 3

(7) *SYSTEM COMPONENT INVENTORY | CENTRALIZED REPOSITORY*

Supplemental C-SCRM Guidance: Organizations may choose to implement centralized inventories that include components from all organizational information systems, networks, and their components. Centralized repositories of inventories provide opportunities for efficiencies in accounting for information systems, networks, and their components. Such repositories may also help organizations to rapidly identify the location and responsible individuals of components that have been compromised,

breached, or are otherwise in need of mitigation actions. The organization should ensure that centralized inventories include supply chain-specific information required for proper component accountability (e.g., supply chain relevance and information system, network, or component owner).

Level(s): 3

(8) *SYSTEM COMPONENT INVENTORY | AUTOMATED LOCATION TRACKING*

Supplemental C-SCRM Guidance: When employing automated mechanisms for tracking of information system components by physical location, the organization should incorporate information system, network, and component tracking needs to ensure accurate inventory.

Level(s): 2, 3

(9) *SYSTEM COMPONENT INVENTORY | ASSIGNMENT OF COMPONENTS TO SYSTEMS*

Supplemental C-SCRM Guidance: When assigning components to systems, the organization should ensure that the information systems and networks with all relevant components are inventoried, marked, and properly assigned. This facilitates quick inventory of all components relevant to information systems and networks and enables tracking of components that are considered critical and require differentiating treatment as part of the information system and network protection activities.

Level(s): 3

CM-9 CONFIGURATION MANAGEMENT PLAN

Supplemental C-SCRM Guidance: Organizations should ensure that C-SCRM is incorporated into the configuration management planning activities. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2, 3.

Control Enhancement(s):

(1) *CONFIGURATION MANAGEMENT PLAN | ASSIGNMENT OF RESPONSIBILITY*

Supplemental C-SCRM Guidance: Organizations should ensure that all relevant roles are defined to address configuration management activities for information systems and networks. Organizations should ensure requirements and capabilities for configuration management are appropriately addressed or included in the following cyber supply chain activities: requirements definition, development, testing, market research and analysis, procurement solicitations and contracts, component installation or removal, system integration, operations, and maintenance.

Level(s): 2, 3

CM-10 SOFTWARE USAGE RESTRICTIONS

Supplemental C-SCRM Guidance: Organizations should ensure that licenses for software used within their information systems and networks are documented, tracked, and maintained. Tracking mechanisms should provide for the ability to trace users and use of licenses to access control information and processes. As an example, when an employee is terminated, a "named user" license, should be revoked and license documentation should be updated to reflect this change.

Level(s): 2, 3

Control Enhancement(s):

(1) *SOFTWARE USAGE RESTRICTIONS | OPEN-SOURCE SOFTWARE*

Supplemental C-SCRM Guidance: When considering software, organizations should review all options and corresponding risks including open source or commercially licensed components. When using open source software (OSS), the organization should understand and review the open source communities' typical procedures regarding provenance, configuration management, sources, binaries, reusable frameworks, reusable libraries' availability for testing and use, and any other information that may impact cyber supply chain risk. Numerous open source solutions are currently in use by organizations, including in integrated development environments (IDEs) and web servers. The organization should:

a. Track the use of OSS and associated documentation;
b. Ensure that the use of OSS adheres to the licensing terms and that these terms are acceptable to the organization
c. Document and monitor the distribution of software as it relates to licensing agreement to control copying and distribution; and
d. Evaluate and periodically audit the OSS's cyber supply chain as provided by the open source developer (e.g., information regarding provenance, configuration management, use of reusable libraries, etc.). This evaluation can be done reasonably easily by the organization through obtaining existing and often public documents as well as using experience based on software update and download processes in which the organization may have participated.

Level(s): 2, 3

CM-11 USER-INSTALLED SOFTWARE

Supplemental C-SCRM Guidance: This control extends to organizational information system and network users who are not employed by the organization. These users may be suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

Level(s): 2, 3

CM-12 INFORMATION LOCATION

Supplemental C-SCRM Guidance: Information residing in different physical locations may be subject to different cyber supply chain risks, depending on the specific location of the information. Components originating or operating from different physical locations may also be subject to different supply chain risks, depending on the specific location of origination or operations. Organizations should manage these risks through limiting access control, specifying allowable or disallowable geographic locations for backup/recovery, patching/upgrades, and information transfer/sharing. NIST SP 800-53 Rev. 5 control enhancement CM-12 (1) is a mechanism that can be used to enable automated location of components.

Level(s): 2, 3

Control Enhancement(s):

(1) *INFORMATION LOCATION | AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION*

Use automated tools to identify organization-defined information on organization-defined system components to ensure controls are in place to protect organizational information and individual privacy.

Level(s): 2, 3

CM-13 DATA ACTION MAPPING

Supplemental C-SCRM Guidance: In addition to personally identifiable information, understanding and documenting a map of system data actions for sensitive or classified information is necessary. Data action mapping should also be conducted to map internet of things (IoT) devices, embedded or stand-alone IoT systems, or IoT System of System data actions. Understanding what classified or IoT information is being processed, its sensitivity and/or effect on a physical thing or physical environment, how the sensitive or IoT information is being processed (e.g., if the data action is visible to an individual or is processed in another part of the system), and by whom provides a number of contextual factors that are important to assessing the degree of risk. Data maps can be illustrated in different ways, and the level of detail may vary based on the mission and business needs of the organization. The data map may be an overlay of any system design artifact that the organization is using. The development of this map may necessitate coordination between program and security personnel regarding the covered data actions and the components that are identified as part of the system.

Level(s): 2, 3

CM-14 SIGNED COMPONENTS

Supplemental C-SCRM Guidance: Organizations should verify that the acquired hardware and software components are genuine and valid by using digitally signed components. Verifying components before allowing installation helps organizations reduce cyber supply chain risks.

Level(s): 3

FAMILY: CONTINGENCY PLANNING

FIPS 200 specifies the Contingency Planning minimum security requirement as follows:

> *Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.*

Cyber supply chain contingency planning includes planning for alternative suppliers of system components, alternative suppliers of systems and services, denial of service attacks to the supply chain, and planning for alternate delivery routes for critical system components. Such contingency plans help ensure existing service providers have an effective continuity of operations pan, especially, when the provider is delivering services in support of a critical mission function. Additionally, many techniques used for contingency planning, such as alternative processing sites, have their own cyber supply chains with their own attendant cyber supply chain risks. Organizations should ensure they understand and manage cyber supply chain risks and dependencies related to the contingency planning activities as necessary.

CP-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: Organizations should integrate C-SCRM into the contingency planning policy and related SCRM Strategy/Implementation Plan, policies, and SCRM Plan. The policy cover information systems and the supply chain network and, at a minimum, address scenarios such as:

a. Unplanned component failure and subsequent replacement;
b. Planned replacement related to feature improvements, maintenance, upgrades, and modernization; and
c. Product and/or service disruption.

Level(s): 1, 2, 3

CP-2 CONTINGENCY PLAN

Supplemental C-SCRM Guidance: Organizations should define and implement a contingency plan for the supply chain information systems and network to ensure preparations are in place to mitigate against the loss or degradation of data or operations. Contingencies should be put in place for the supply chain, network and information systems (especially critical components), and processes to ensure protection against compromise, provide appropriate failover, and timely recovery to an acceptable state of operations.

Level(s): 2, 3

Control Enhancement(s):

(1) *CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*

Supplemental C-SCRM Guidance: Coordinate contingency plan development for supply chain risks with organizational elements responsible for related plans.

Level(S): 2, 3

(2) *CONTINGENCY PLAN | CAPACITY PLANNING*

Supplemental C-SCRM Guidance: This enhancement helps availability of the supply chain network or information system components.

Level(s): 2, 3

(7) *CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS*

Supplemental C-SCRM Guidance: Organizations should ensure that supply chain network, information systems and components provided by an external service provider have appropriate failover (to include personnel, equipment, and network resources) to reduce or prevent service interruption or ensure timely recovery. Organizations should ensure that contingency planning requirements are defined as part of the service-level agreement. The agreement may have specific terms addressing critical components and functionality support in case of denial of service to ensure continuity of operation. Organizations should coordinate with external service providers to identify service providers' existing contingency plan practices and build on them as required by the organization's mission and business needs. Such coordination will aid in cost reduction and efficient implementation. Organizations should require its prime contractors that provide a mission/business-critical or -enabling service or product to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 3

(8) *CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*

Supplemental C-SCRM Guidance: Ensure that critical assets (including hardware, software, and personnel) are identified to ensure that appropriate contingency planning requirements are defined and applied to ensure continuity of operation. A key step in this process is to complete a criticality analysis on components, functions, and processes to identify all critical assets. See Section 2 and NISTIR 8179 for additional guidance on criticality analyses.

Level(s): 3

CP-3 CONTINGENCY TRAINING

Supplemental C-SCRM Guidance: Organizations should ensure that critical suppliers are included in contingency training.

Level(s): 2, 3

Control Enhancement(s):

(1) *CONTINGENCY TRAINING | SIMULATED EVENTS*

Supplemental C-SCRM Guidance: Organizations should ensure that suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers who have roles and responsibilities in providing critical services are included in contingency training exercises.

Level(s): 3

CP-4 CONTINGENCY PLAN TESTING

Supplemental C-SCRM Guidance: Organizations should ensure that critical suppliers are included in contingency testing. The organization, in coordination with the service provider(s) should test whether continuity/resiliency capabilities, such as failover from a primary production site to a back-up site. perform as required. This testing may occur separately from a training exercise or be performed during the exercise. Organizations should reference their C-SCRM threat assessment output to develop scenarios to test how well the organization is able to withstand and/or recover from a C-SCRM threat event.

Level(s): 2, 3

CP-6 ALTERNATE STORAGE SITE

Supplemental C-SCRM Guidance: When managed by suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, alternate storage sites are considered within an organization's cyber supply chain network. Organizations should apply appropriate cyber supply chain controls to those storage sites.

Level(s): 2, 3

Control Enhancement(s):

(1) *ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*

Supplemental C-SCRM Guidance: This enhancement helps resiliency of supply chain network, information systems, and information system components.

Level(s): 2, 3

CP-7 ALTERNATE PROCESSING SITE

Supplemental C-SCRM Guidance: When managed by suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, alternate storage sites are considered within an organization's cyber supply chain. Organizations should apply appropriate cyber supply chain controls to those processing sites.

Level(s): 2, 3

CP-8 TELECOMMUNICATIONS SERVICES

Supplemental C-SCRM Guidance: Organizations should incorporate alternate telecommunication service providers for their cyber supply chain and to support critical information systems.

Level(s): 2, 3

Control Enhancement(s):

(3) *TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS*

Supplemental C-SCRM Guidance: Separation of primary and alternate providers supports cyber supply chain resilience.

Level(s): 2, 3

(4) *TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*

Supplemental C-SCRM Guidance: For C-SCRM, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers contingency plans should provide separation in infrastructure, service, process, and personnel, where appropriate.

Level(s): 2, 3

CP-11 ALTERNATE COMMUNICATIONS PROTOCOLS

3392 Supplemental C-SCRM Guidance: Organizations should ensure critical suppliers are included in
3393 contingency plans, training, and testing as part of incorporating alternate communications protocol
3394 capability to establish supply chain resilience.
3395
3396 Level(s): 2, 3
3397

FAMILY: IDENTIFICATION AND AUTHENTICATION

FIPS 200 specifies the Identification and Authentication minimum security requirement as follows:

> *Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.*

NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations,* expands the FIPS 200 identification and authentication control family to include identification and authentication of components, in addition to individuals (users) and processes acting on behalf of individuals within the cyber supply chain network. Identification and authentication is critical to C-SCRM because it provides traceability of individuals, processes acting on behalf of individuals, and specific systems/components in an organization's cyber supply chain network. Identification and authentication is required to appropriately manage cyber supply chain risks to both reduce risks of cyber supply chain compromise and to generate evidence in case of cyber supply chain compromise.

IA-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: The organization should, at organizationally-defined intervals, review, enhance, and update their identity and access management policies and procedures to ensure that critical roles and processes within the supply chain network are defined and that the organization's critical systems, components, and processes are identified for traceability. This should include the identity of critical components that may not have been considered under identification and authentication in the past. Note that providing identification for all items within the supply chain would be cost-prohibitive, and discretion should be used. The organization should update related C-SCRM Strategy/Implementation Plan(s), Policies, and C-SCRM Plans.

Level(s): 1, 2, 3

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Supplemental C-SCRM Guidance: Organizations should ensure that identification and requirements are defined and applied for organizational users accessing an ICT/OTsystem or supply chain network. An organizational user may include employees as well as individuals deemed to have the equivalent status of employees (e.g., contractors, guest researchers, etc.) and may include system integrators fulfilling contractor roles. Criteria such as "duration in role" can aid in defining which identification and authentication mechanisms are used. The organization may choose to define a set of roles and associate a level of authorization to ensure proper implementation.

Level(s): 1, 2, 3

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Supplemental C-SCRM Guidance: Organizations should implement capabilities to distinctly and positively identify devices and software within their supply chain and, once identified, be able to verify that the identity is authentic. Devices that require unique device-to-device identification and authentication should

be defined by type, by device, or by a combination of type and device. Software that requires authentication should be identified through a software identification tag (SWID) that enables verification of the software package and authentication of the organization releasing the software package.

Level(s): 1, 2, 3

IA-4 IDENTIFIER MANAGEMENT

Supplemental C-SCRM Guidance: Identifiers allow for greater discoverability and traceability. Within the organization's cyber supply chain, identifiers should be assigned to systems, individuals, documentation, devices, and components. In some cases, identifiers may be maintained throughout a system's life cycle, from concept to retirement, but at a minimum throughout the system's life within the organization.

For software development, identifiers should be assigned for those components that have achieved configuration item recognition. For devices and operational systems, identifiers should be assigned when the items enter the organization's supply chain, such as when they are transferred to the organization's ownership or control through shipping and receiving or via download.

Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers typically use their own identifiers for tracking purposes within their own supply chain. Organizations should correlate those identifiers with the organization-assigned identifiers for traceability and accountability.

Level(s): 2, 3

Related Controls: IA-3 (1), IA-3 (2), IA-3 (3), and IA-3 (4)

Control Enhancement(s):

(6) *IDENTIFIER MANAGEMENT | CROSS-ORGANIZATION MANAGEMENT*

Supplemental C-SCRM Guidance: This enhancement helps traceability and provenance of elements within the cyber supply chain, through the coordination of identifier management among the organization and its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. This includes information systems and components as well as individuals engaged in supply chain activities.

Level(s): 1, 2, 3

IA-5 AUTHENTICATOR MANAGEMENT

Supplemental C-SCRM Guidance: This control facilitates traceability and non-repudiation throughout the cyber supply chain.

Level(s): 2, 3

Control Enhancement(s):

(5) *AUTHENTICATOR MANAGEMENT | CHANGE AUTHENTICATORS PRIOR TO DELIVERY*

Supplemental C-SCRM Guidance: This enhancement provides verification of chain of custody within the organization's cyber supply chain.

Level(s): 3

(9) *AUTHENTICATOR MANAGEMENT | FEDERATED CREDENTIAL MANAGEMENT*

Supplemental C-SCRM Guidance: This enhancement facilitates provenance and chain of custody within the organization's cyber supply chain.

Level(s): 3

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Supplemental C-SCRM Guidance: Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers have the potential to engage the organization's supply chain for service delivery (development/integration services, product support, etc.). Organizations should manage the establishment, auditing, use, and revocation of identification credentials and authentication of non-organizational users within the \ supply chain. Organizations should ensure promptness in performing identification and authentication activities, especially in the case of revocation management, to help mitigate against cyber supply chain risks such as insider threat.

Level(s): 2, 3

IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION

Supplemental C-SCRM Guidance: Organizations should ensure that identification and authentication is defined and managed for access to services (i.e., web applications using digital certificates or services or applications that query a database as opposed to labor-services) throughout the supply chain. Organizations should ensure they know what services are being procured and from whom. Services procured should be listed on a validated list of services for the organization or have compensating controls in place.

Level(s): 2, 3

FAMILY: INCIDENT RESPONSE

FIPS 200 specifies the Incident Response minimum security requirement as follows:

> *Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.*

Cyber supply chain compromises may span suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Organizations should ensure their incident response controls address C-SCRM including what, when and how information about incidents will be reported or shared by, with, or between suppliers, developers, system integrators, external system service providers, other ICT/OT-related service providers, and any relevant interagency bodies. Incident response will help determine whether an incident is related to the cyber supply chain.

IR-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: Organizations should integrate C-SCRM into incident response policy and procedures, and related C-SCRM Strategy/Implementation Plan(s), Policies, and C-SCRM Plan. Policy and procedures must provide direction about how to address supply chain related incidents and those cybersecurity incidents that may complicate or impact the cyber supply chain. Individuals working within specific mission and system environments need to recognize cyber supply chain-related incidents. Incident response policy should state when and how threats and incidents should be handled, reported, and managed.

Additionally, the policy should define when, how, and with whom to communicate to the FASC (Federal Acquisition Security Council), and other stakeholders or partners within the broader supply chain in the event of a cyber threat or incident. Departments and agencies must notify the FASC of supply chain risk information when 1) the FASC requests information relating to a particular source, covered article or procures; or 2) an executive agency has determined there is a reasonable basis to conclude a substantial supply chain risk associated with a source, covered procurement, or covered article exists. In such instances, the executive agency shall provide the FASC with relevant information concerning the source or covered article, including: (i) supply chain risk information identified through the course of the agency's activities in furtherance of mitigating, identifying or managing its supply chain risk; and (ii) supply chain risk information regarding covered procurement actions by the agency under the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) 41 U.S.C. § 4713; and any orders issued by the agency under 41 U.S.C. § 4713. Bidirectional communication with supply chain partners should be defined in agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to inform all involved parties of a cyber supply chain incident. Incident information may also be shared with organizations such as the Federal Bureau of Investigation (FBI), US CERT (United States Computer Emergency Readiness Team), and the NCCIC (National Cybersecurity and Communications Integration Center) as appropriate. Depending on the severity of the incident, the need for accelerated communications up and down the supply chain may be necessary. Appropriate agreements should be put in place with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to ensure speed of communication, response, corrective actions, and other related activities. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

In Levels 2 and 3, procedures and organization-specific incident response methods must be in place, training completed (consider including Operations Security (OPSEC) and any appropriate threat briefing in training), and coordinated communication established throughout the supply chain to ensure an efficient and coordinated incident response effort.

Level(s): 1, 2, 3

Control Enhancement(s):

(1) *POLICY AND PROCEDURES | C-SCRM INCIDENT INFORMATION SHARING*

Organizations should ensure that their incident response policies and procedures provide guidance on effective information sharing of incidents and other key risk indicators in the cyber supply chain. Guidance should at a minimum cover the collection, synthesis, and distribution of incident information from a diverse set of data sources such as publicly data repositories, paid subscription services, and in-house threat intelligence teams.

Organizations operating in the public sector should include specific guidance on when and how to communicate with interagency partnerships such as the FASC (Federal Acquisition Security Council) and other stakeholders or partners within the broader supply chain in the event of a cyber threat or incident.

Departments and agencies must notify the FASC of supply chain risk information when
1) The FASC requests information relating to a particular source, covered article or procures; or
2) An executive agency has determined there is a reasonable basis to conclude a substantial supply chain risk associated with a source, covered procurement, or covered article exists.

In such instances, the executive agency shall provide the FASC with relevant information concerning the source or covered article, including:
i. Supply chain risk information identified through the course of the agency's activities in furtherance of mitigating, identifying or managing its supply chain risk; and
ii. Supply chain risk information regarding covered procurement actions by the agency under the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) 41 U.S.C. § 4713; and any orders issued by the agency under 41 U.S.C. § 4713.

Level(s): 1, 2, 3

IR-2 INCIDENT RESPONSE TRAINING

Supplemental C-SCRM Guidance: Organizations should ensure that critical suppliers are included in incident response training.

Level(s): 2, 3

IR-3 INCIDENT RESPONSE TESTING

Supplemental C-SCRM Guidance: Organizations should ensure that critical suppliers are included in and/or provided incident response testing.

Level(s): 2, 3

IR-4 INCIDENT HANDLING

Supplemental C-SCRM Guidance: C-SCRM-specific supplemental guidance provided in control enhancements.

Level(s): 1,2,3

Control Enhancement(s):

(6) *INCIDENT HANDLING | INSIDER THREATS*

Supplemental C-SCRM Guidance: This enhancement helps limit exposure of the C-SCRM information systems, networks, and processes to insider threats. Organizations should ensure that insider threat incident handling capabilities account for the potential of insider threats associated with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers' personnel with access to ICT/OT systems within the authorization boundary.

Level(s): 1, 2, 3

(7) *INCIDENT HANDLING | INSIDER THREATS - INTRA-ORGANIZATION*

Supplemental C-SCRM Guidance: This enhancement helps limit exposure of C-SCRM information systems, networks, and processes to insider threats. Organizations should ensure that insider threat coordination includes suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

Level(s): 1, 2, 3

(10) *INCIDENT HANDLING | SUPPLY CHAIN COORDINATION*

Supplemental C-SCRM Guidance: A number of organizations may be involved in managing incidents and responses for supply chain security. After an initial processing of the incident is completed and a decision is made to take action (in some cases, the action may be "no action"), the organization may need to coordinate with their suppliers, developers, system integrators, external system service providers, other ICT/OT-related service providers, and any relevant interagency bodies to facilitate communications, incident response, root cause, and corrective actions activities. Organizations should securely share information through a coordinated set of personnel in key roles to allow for a more comprehensive incident handling approach. Selecting suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers with mature capabilities for supporting cyber supply chain incident handling is important for reducing cyber supply chain risk. If transparency for incident handling is limited due to the nature of the relationship, define a set of acceptable criteria in the agreement (e.g., contract). A review (and potential revision) of the agreement is recommended, based on the lessons learned from previous incidents. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2

(11) *INCIDENT HANDLING | INTEGRATED INCIDENT RESPONSE TEAM*

Supplemental C-SCRM Guidance: An organization should include a forensics team and/or capability as part of an integrated incident response team for supply chain incidents. Where relevant and practical, integrated incident response teams should also include necessary geographical representation as well as suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

Level(s): 3

IR-5 INCIDENT MONITORING

Supplemental C-SCRM Guidance: Organizations should ensure agreements with suppliers include requirements to track and document incidents and response decisions and activities.

Level(s): 2, 3

IR-6 INCIDENT REPORTING

Supplemental C-SCRM Guidance: C-SCRM-specific supplemental guidance provided in control enhancement IR-6 (3).

Level(s): 3

Control Enhancement(s):

(3) *INCIDENT REPORTING | SUPPLY CHAIN COORDINATION*

Supplemental C-SCRM Guidance: Communications of security incident information from the organization to suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers or vice-verse requires protection. The organization should ensure that information is reviewed and approved for sending based on its agreements with the suppliers and any relevant interagency bodies. Any escalation of or exception from this reporting should be clearly defined in the agreement. The organization should ensure that incident reporting data is adequately protected for transmission and received by approved individuals only. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 3

IR-7 INCIDENT RESPONSE ASSISTANCE

Supplemental C-SCRM Guidance: C-SCRM-specific supplemental guidance provided in control enhancement IR-7 (2).

Level(s): 3

Control Enhancement(s):

(1) *INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS*

Supplemental C-SCRM Guidance: Organization's agreements with prime contractors should specify the conditions under which a government-approved or -designated third party will be available or may be required to provide assistance with incident response, as well as describe the role and responsibility of that third party.

Level(s): 3

IR-8 INCIDENT RESPONSE PLAN

Supplemental C-SCRM Guidance: Organizations should coordinate, develop, and implement an incident response plan that includes information sharing responsibilities with critical suppliers and, in a federal context, interagency partners and the FASC. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Related Control(s): IR-10

Level(s): 2, 3

IR-9 INFORMATION SPILLAGE RESPONSE

Supplemental C-SCRM Guidance: The supply chain is vulnerable to information spillage. The organization should include supply chain-related information spills in its information spillage response plan. This may require coordination with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The details of how this coordination is to be conducted should be included in the agreement (e.g., contract). Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 3

Related Controls: SA-4

FAMILY: MAINTENANCE

FIPS 200 specifies the Maintenance minimum security requirement as follows:

> *Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.*

Maintenance is frequently performed by an entity that is separate from the organization. As such, maintenance becomes part of the supply chain. Maintenance includes performing updates and replacements. C-SCRM should be applied to maintenance situations including assessing the cyber supply chain risks, selecting C-SCRM controls, implementing these controls, and monitoring them for effectiveness.

MA-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: Organizations should ensure that C-SCRM is included in maintenance policies and procedures, and related SCRM Strategy/Implementation Plan, SCRM Policies, and SCRM Plan(s) for all organizational information systems and networks. With many maintenance contracts, information on mission, organization, and system-specific objectives and requirements is shared between the organization and its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, allowing for vulnerabilities and opportunities for attack. In many cases, the maintenance of systems is outsourced to a system integrator and as such, appropriate measures must be taken. Even when maintenance is not outsourced, the upgrades and patches, frequency of maintenance, replacement parts, and other aspects of system maintenance are affected by the supply chain.

Maintenance policies should be defined both for the system and the network. The maintenance policy should reflect controls based on a risk assessment (including criticality analysis), including controls such as remote access, roles and attributes of maintenance personnel that have access, the frequency of updates, duration of contract, logistical path and method used for updates or maintenance, and monitoring and audit mechanisms. The maintenance policy should state which tools are explicitly allowed or not allowed. For example, in the case of software maintenance, source code, test cases, and other item accessibility to maintain a system or components should be stated in the contract.

Maintenance policies should be refined and augmented at each level. At Level 1, the policy should explicitly assert that C-SCRM should be applied throughout the SDLC, including maintenance activities. At Level 2, the policy should reflect the mission operation's needs and critical functions. At Level 3 it should reflect the specific system needs. The requirements in Level 1, such as nonlocal maintenance, should flow to Levels 2 and 3; for example, when nonlocal maintenance is not allowed by Level 1, it should also not be allowed at Levels 2 and 3.

The organization should communicate applicable maintenance policy requirements to relevant prime contractors and require they implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 1, 2, 3

MA-2 CONTROLLED MAINTENANCE

Supplemental C-SCRM Guidance: C-SCRM-specific supplemental guidance is provided in control enhancement MA-2 (2).

Control Enhancement(s):

(2) *CONTROLLED MAINTENANCE |AUTOMATED MAINTENANCE ACTIVITIES*

Supplemental C-SCRM Guidance: Organizations should ensure that all automated maintenance activities for supply chain systems and networks are controlled and managed according to the maintenance policy. Examples of automated maintenance activities can include COTS product patch updates, call home features with failure notification feedback, etc. Managing these activities may require establishing staging processes with appropriate supporting mechanisms to provide vetting or filtering as appropriate. Staging processes may be especially important for critical systems and components.

Level(s): 3

MA-3 MAINTENANCE TOOLS

Supplemental C-SCRM Guidance: Maintenance tools are considered part of the supply chain. They also have a supply chain of their own. C-SCRM should be integrated when the organization acquires or upgrades a maintenance tool (e.g., an update to development environment or testing tool), including during the selection, ordering, storage, and integration of the maintenance tool. The organization should perform continuous review and approval of maintenance tools, to include those maintenance tools in use by external service providers. The organization should also integrate C-SCRM when evaluating replacement parts for maintenance tools. This control may be performed at both Levels 2 and 3, depending on how an agency handles the acquisition, operations, and oversight of maintenance tools.

Level(s): 2, 3.

Control Enhancement(s):

(1) *MAINTENANCE TOOLS | INSPECT TOOLS*

Supplemental C-SCRM Guidance: The organization should deploy acceptance testing to verify that the maintenance tools of the ICT supply chain infrastructure are as expected. Maintenance tools should be authorized with appropriate paperwork, verified as claimed through initial verification, and tested for vulnerabilities, appropriate security configurations, and stated functionality.

Level(s): 3

(2) *MAINTENANCE TOOLS | INSPECT MEDIA*

Supplemental C-SCRM Guidance: The organization should verify that the media containing diagnostic and test programs that suppliers use on the organization's information systems operate as expected and provide only required functions. Use of media from maintenance tools should be consistent with organization's policies and procedures and pre-approved. Organizations should also ensure the functionality does not exceed that which was agreed upon.

Level(s): 3

(3) *MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL*

Supplemental C-SCRM Guidance: Unauthorized removal of systems and network maintenance tools from the cyber supply chain may introduce supply chain risk including, for example, unauthorized modification, replacement with counterfeit, or malware insertion while the tool is outside of the organization's control. Systems and network maintenance tools can include integrated development environment (IDE), testing, or vulnerability scanning. For C-SCRM, it is important that organizations

should explicitly authorize, track, and audit any removal of maintenance tools. Once systems and network tools are allowed access to an organization/information system, they should remain the property/asset of the system owner and tracked if removed and used elsewhere in the organization. ICT maintenance tools either currently in use or in storage should not be allowed to leave the organization's premises until they are properly vetted for removal (i.e., maintenance tool removal should not exceed in scope what was authorized for removal, and should be completed in accordance with the organization's established policies and procedures).

Level(s): 3

MA-4 NONLOCAL MAINTENANCE

Supplemental C-SCRM Guidance: Nonlocal maintenance may be provided by contractor personnel. Appropriate protections should be in place to manage associated risks. Controls applied to internal maintenance personnel are applied to any suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers performing a similar maintenance role and enforced through contractual agreements with their external service providers.

Level(s): 2, 3

Control Enhancement(s):

(3) *NONLOCAL MAINTENANCE | COMPARABLE SECURITY AND SANITIZATION*

Supplemental C-SCRM Guidance: Should any nonlocal maintenance or diagnostic services be performed to systems components or systems by suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, the organization should ensure that:

- Appropriate measures are taken to verify that the nonlocal environment meets appropriate security levels for maintenance and diagnostics per agreements between the organization and vendor;
- Appropriate levels of sanitizing are completed to remove any organization-specific data residing in components; and
- Appropriate diagnostics are completed to ensure that components are sanitized, preventing malicious insertion prior to returning to the organizational system and or supply chain network.

The organization should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2, 3

MA-5 MAINTENANCE PERSONNEL

Supplemental C-SCRM Guidance: Maintenance personnel may be employed by a supplier, developer, system integrators, external system service providers, or other ICT/OT-related service providers. As such, appropriate protections should be in place to manage associated risks. The same controls applied to internal maintenance personnel should be applied to any contractor personnel performing a similar maintenance role and enforced through contractual agreements with their external service providers.

Level(s): 2, 3

Control Enhancement(s):

(4) *MAINTENANCE PERSONNEL | FOREIGN NATIONALS*

Supplemental C-SCRM Guidance: Vetting of foreign nationals with access to critical non-national security systems/services must take C-SCRM into account and be extended to all relevant contractor personnel. Organizations should specify in agreements any restrictions or vetting requirements that pertain to foreign nationals and flow requirement down to relevant sub-contractors.

Level(s): 2, 3

MA-6 TIMELY MAINTENANCE

Supplemental C-SCRM Guidance: For spare parts, replacement parts, or alternate sources, the organization should purchase through original equipment manufacturers (OEMs), authorized distributors or authorized reseller and ensure appropriate lead times. If OEMs are not available, it is preferred to acquire from authorized distributors. If an OEM or an authorized distributor is not available, then it is preferred to acquire from an authorized reseller. Organizations should obtain verification on whether the distributor or reseller is authorized. Where possible, organizations should use an authorized distributor/dealer approved list. If the only alternative is to purchase from a non-authorized distributor or secondary market, a risk assessment should be performed, including a revisit of criticality and threat analysis to identify additional risk mitigations to be used. For example, the organization should check the source of supply for history of counterfeits, inappropriate practices, or a criminal record. See Section 2 for criticality and threat analysis details. The organization should maintain a bench stock of critical OEM parts, if feasible, when acquisition of such parts may not be able to be accomplished within needed timeframes.

Level(s): 3

MA-7 FIELD MAINTENANCE

Supplemental C-SCRM Guidance: Organizations should use trusted facilities when additional rigor and quality control checks are needed, if at all practical or possible. Trusted facilities should be on an approved list and have additional controls in place.

Related Control(s): MA-2, MA-4, MA-5.

Level(s): 3

MA-8 MAINTENANCE MONITORING AND INFORMATION SHARING (NEW)

Control: The organization monitors the status of systems and components, and communicates out-of-bounds and out-of-spec performance to suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The organization should also report this information to the Government-Industry Data Exchange Program (GIDEP).

Supplemental C-SCRM Guidance: Tracking failure rates of components provides useful information to the acquirer to help plan for contingencies, alternate sources of supply, and replacements. Failure rates are also useful for monitoring quality and reliability of systems and components. This information provides useful feedback to suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers for corrective action and continuous improvement. In Level 2, agencies should track and communicate the failure rates to suppliers (OEM and/or an authorized distributor). The failure rates and the issues that can indicate failures including root causes should be identified by an organization's technical personnel (e.g., developers, administrators, or maintenance engineers) in Level 3 and communicated to Level 2. These individuals are able to verify the problem and identify technical alternatives.

Related Control(s): IR-4(10).

Level(s): 3

FAMILY: MEDIA PROTECTION

FIPS 200 specifies the Media Protection minimum security requirement as follows:

> *Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.*

Media itself can be a component traversing the cyber supply chain or containing information about the organization's cyber supply chain. This includes both physical and logical media including, for example, system documentation on paper or in electronic files, shipping and delivery documentation with acquirer information, memory sticks with software code, or complete routers or servers that include permanent media. The information contained on the media may be sensitive or proprietary information. Additionally, the media is used throughout the SDLC, from concept to disposal. Organizations should ensure that Media Protection controls are applied to both an organization's media and the media received from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers throughout the SDLC.

MP-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: Various documents and information on a variety of physical and electronic media are disseminated throughout the cyber supply chain. This information may contain a variety of sensitive information and intellectual property from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers and should be appropriately protected. Media protection policies and procedures should address cyber supply chain concerns including media in the organization's cyber supply chain, as well as media throughout the SDLC.

Level(s): 1, 2

MP-4 MEDIA STORAGE

Supplemental C-SCRM Guidance: Media storage controls should include C-SCRM activities. Organizations should specify and include in agreements (e.g., contracting language) media storage policies for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The organization should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 1, 2

MP-5 MEDIA TRANSPORT

Supplemental C-SCRM Guidance: The organization should incorporate C-SCRM activities when media is transported, either by organizational or non-organizational personnel. Some of the techniques to protect media during transport and storage include cryptographic techniques and approved custodian services.

Level(s): 1, 2

MP-6 MEDIA SANITIZATION

Supplemental C-SCRM Guidance: Organizations should specify and include in agreements (e.g., contracting language) media sanitization policies for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Media is used throughout the SDLC. Media traversing or residing in the cyber supply chain may originate anywhere including from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. It can be new, refurbished, or reused. Media sanitization is critical to ensure that information is removed before the media is used, reused, or discarded. For media containing privacy or other sensitive information (e.g. CUI), the organization should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2, 3

Related Controls: MP-6(1), MP-6(2), MP-6(3), MP-6(7), MP-6(8)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

FIPS 200 specifies the Physical and Environmental Protection minimum security requirement as follows:

> *Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.*

Cyber supply chains span the physical and logical world. Physical factors include, for example, weather and road conditions that may have an impact on transporting cyber components (or devices) from one location to another between persons or organizations within a supply chain. If not properly addressed as a part of the C-SCRM risk management processes, physical and environmental risks may have a negative impact on the organization's ability to receive critical components in a timely manner, which may in turn impact their ability to perform mission operations. Organizations should require implementation of appropriate physical and environmental control within their supply chain.

PE-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: The organization should integrate C-SCRM practices and requirements into physical and environmental protection policy and procedures. The degree of protection should be commensurate with the degree of integration. The physical and environmental protection policy should ensure that the physical interfaces of the cyber supply chain have adequate protection and audit for such protection.

Level(s): 1, 2, 3

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Supplemental C-SCRM Guidance: Organizations should ensure only authorized individuals with a need for physical access have access to information or systems (e.g., sensitive or classified). Such authorizations should specify what the individual is permitted or not permitted to do with regard to their physical access (e.g. view, alter/configure, insert something, connect something, remove, etc.). Agreements should address physical access authorization requirements and the organization should require its prime contractors to implement this control, flowing down this requirement to relevant sub-tier contractors. Authorization for non-Federal employees should follow an approved protocol, which includes documentation of the authorization, to include specifying any prerequisites or constraints that pertain to such authorization (e.g., individual must be escorted by a Federal employee, individual must be badged, individual is permitted physical access during normal business hours, etc.).

Level(s): 2, 3

Control Enhancement(s):

(1) *PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION OR ROLE*

Supplemental C-SCRM Guidance: Role-based authorizations for physical access should include federal (e.g., agency/department employees) and non-federal employees (e.g., suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers). When role-based authorization is used, the type and level of access allowed for that role or position must be pre-established and documented.

Level(s): 2, 3

PE-3 PHYSICAL ACCESS CONTROL

Supplemental C-SCRM Guidance: Physical access control should include individuals and organizations engaged in the organization's cyber supply chain. A vetting process should be in place based on organizational-defined requirements and policy prior to granting access to the cyber supply chain infrastructure and any relevant elements. Access establishment, maintenance, and revocation processes should meet organizational access control policy rigor. The speed of revocation for suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers needing access to physical facilities should be managed in accordance with the activities performed in their contracts. Prompt revocation is critical when either individual or organizational need no longer exists.

Level(s): 2, 3

Control Enhancement(s):

(1) *PHYSICAL ACCESS CONTROL | SYSTEM ACCESS*

Supplemental C-SCRM Guidance: Physical access controls should be extended to contractor personnel. Any contractor resources providing services support with physical access to the cyber supply chain infrastructure and any relevant elements should adhere to access controls. Policies and procedures should be consistent with those applied to employee personnel with similar levels of physical access.

Level(s): 2, 3

(2) *PHYSICAL ACCESS CONTROL | FACILITY AND SYSTEMS*

Supplemental C-SCRM Guidance: When determining the extent, frequency, and/or randomness of facility security checks of facilities, organizations should account for exfiltration risks resulting from covert listening devices. Such devices may include wiretaps, roving bugs, cell site simulators, and other eavesdropping technologies that can transfer sensitive information out of organizations.

Level(s): 2, 3

(5) *PHYSICAL ACCESS CONTROL | TAMPER PROTECTION*

Supplemental C-SCRM Guidance: Tamper protection is critical for reducing cyber supply chain risks in products. The organization should implement validated tamper protections techniques within the cyber supply chain. For critical products, the organization should require and assess whether and to what extent a supplier has implemented tamper protection mechanism. The assessment may also include whether and how such mechanisms are required and applied by the supplier's upstream supply chain entities.

Level(s): 2, 3

PE-6 MONITORING PHYSICAL ACCESS

Supplemental C-SCRM Guidance: Individuals physically accessing the organization's facilities, information, or physical asset(s), including via the cyber supply chain, may be employed by the organization's employees, on-site or remotely located contractors, visitors, other third parties (e.g., maintenance personnel under contract with the contractor organization), or an individual affiliated with an organization in the upstream supply chain. The organization should monitor these individuals' activities to reduce associated cyber supply chain risks or require monitoring in agreements.

Level(s): 1, 2, 3

PE-16 DELIVERY AND REMOVAL

Supplemental C-SCRM Guidance: This control enhancement reduces cyber supply chain risks introduced during the physical delivery and removal of hardware components from the organization's information systems or cyber supply chain.

Level(s): 3

PE-17 ALTERNATE WORK SITE

Supplemental C-SCRM Guidance: The organization should incorporate protections to guard against cyber supply chain risks associated with organizational employees or contractor personnel within or accessing the supply chain infrastructure using alternate work sites. This can include third party personnel who may also work from alternate worksites.

Level(s): 3

PE-18 LOCATION OF SYSTEM COMPONENTS

Supplemental C-SCRM Guidance: Physical and environmental hazards or disruptions have an impact on the availability of products that are or will be acquired and physically transported to the organization's locations. For example, organizations should incorporate the manufacturing, warehousing, or distribution location of information system components critical for agency operations when planning for alternative suppliers for these components.

Level(s): 1, 2, 3

Related Controls: CP-6, CP-7

PE-20 ASSET MONITORING AND TRACKING

Supplemental C-SCRM Guidance: The organization should, whenever possible and practical, use asset location technologies to track system and components transported between entities across the supply chain, between protected areas, or in storage awaiting implementation, testing, maintenance, or disposal. Methods include RFID, digital signatures, or blockchains. These technologies help protect against:

a. Diverting system or component for counterfeit replacement;
b. Loss of confidentiality, integrity, or availability of system or component function and data (including data contained within the component and data about the component); and
c. Interrupting supply chain and logistics processes for critical components. In addition to providing protection capabilities, asset location technologies also help gather data that can be used for incident management.

Level(s): 2, 3

PE-23 FACILITY LOCATION

Supplemental ICT SCRM Guidance: Organizations should incorporate Facility Location when assessing risk associated with suppliers. Factors may include geographic location (e.g., Continental United States (CONUS), Outside the Continental United States (OCONUS)), physical protections in place at one or more of the relevant facilities, local management and control of such facilities, environmental hazard potential (e.g., Located in a high risk seismic zone), and alternative facility locations. For critical vendors or products, organizations should specifically address any requirements or restrictions concerning the vendors (or their upstream supply chain providers) facility locations in contracts and flow down this requirement to relevant sub-level contractors.

Level(s): 2, 3

Related Controls: SA-9(8)

FAMILY: PLANNING

FIPS 200 specifies the Planning minimum security requirement as follows:

> *Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.*

C-SCRM should influence security planning, including such activities as security architecture, coordination with other organizational entities, and development of System Security Plans. When acquiring products and services from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, organizations may be sharing facilities with those organizations, have employees of these entities on the organization's premises, or use information systems that belong to those entities. In these and other applicable situations, organizations should coordinate their security planning activities with these entities to ensure appropriate protection of an organization's processes, information systems, as well as of the systems and components traversing the cyber supply chain. When establishing security architectures, organizations should provide for component and supplier diversity to manage the cyber supply chain risks to include suppliers going out of business or stopping the production of specific components. Finally, as stated in Section 2 and Appendix C, organizations should integrate C-SCRM controls into their Risk Response Frameworks (Levels 1 and 2) as well as C-SCRM Plans (Level 3).

PL-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: Security planning policy and procedures should integrate C-SCRM. This includes creating, disseminating, and updating security policy, operational policy, and procedures for C-SCRM to shape acquisition or development requirements and the follow-on implementation, operations, and maintenance of systems and system interfaces and network connections. The C-SCRM policy and procedures provide inputs into and take guidance from C-SCRM Strategy & Implementation Plan at Level 1. The C-SCRM policy and procedures provide guidance to and take inputs from System Security Plan and C-SCRM Plan at Level 3. In Level 3, ensure that the full SDLC is covered from the C-SCRM perspective.

Level(s): 2

Related Controls: PL-2, PM-30

PL-2 SYSTEM SECURITY AND PRIVACY PLANS

Supplemental C-SCRM Guidance: The system security plan (SSP) should integrate C-SCRM. The organization may choose to develop a stand-alone C-SCRM plan for an individual system or integrate SCRM controls into their SSP. The system security plan and/or system-level C-SCRM plan provide inputs into and take guidance from the C-SCRM Strategy & Implementation Plan at Level 1 and C-SCRM policy at Levels 1 and 2. In addition to coordinating within the organization, the organization should coordinate with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to develop and maintain their SSPs. For example, building and operating a system requires a significant amount of coordination and collaboration between the organization and system integrator personnel. Such coordination and collaboration should be addressed in the system security plan

or stand-alone C-SCRM plan. These plans should also take into account that suppliers or external service providers may not be able to customize to the acquirer's requirements. It is recommended that suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers also develop C-SCRM plans for non-federal (i.e., contractor) systems that are processing federal agency information, and flow down this requirement to relevant sub-level contractors.

Section 2, Appendix C, and Appendix D provide guidance on C-SCRM strategy, policy, and plan. Controls in this publication (NIST SP 800-161 Rev. 1) should be used for the C-SCRM portion of the SSP.

Level(s): 3

Related Controls: PM-30

PL-4 RULES OF BEHAVIOR

Supplemental C-SCRM Guidance: Rules of behavior apply to contractor personnel as well as to internal agency personnel. Contractor organizations are responsible for ensuring that their employees follow applicable rules of behavior. Individual contractors should not be granted access to agency systems or data until they have acknowledged and demonstrated compliance with this control. Failure to meet this control can result in removal of access for such individuals.

Level(s): 2, 3

PL-7 CONCEPT OF OPERATIONS

Supplemental C-SCRM Guidance: Concept of operations (CONOPS) should describe how the organization intends to operate the system from the perspective of C-SCRM. It should integrate C-SCRM and be managed and updated throughout the SDLC to address cyber supply chain risks to the applicable system.

Level(s): 3

PL-8 SECURITY AND PRIVACY ARCHITECTURES

Supplemental C-SCRM Guidance: Security and privacy architecture defines and directs implementation of security and privacy-protection methods, mechanisms, and capabilities to the underlying systems and networks, as well as the information system that is being created. Security architecture is fundamental to C-SCRM because it helps to ensure security is built-in throughout the SDLC. Organizations should consider implementing zero-trust architectures. organization should also ensure that the security architecture is well understood by system developers/engineers and system security engineers. This control applies to both federal agency and non-federal agency employees.

Level(s): 2, 3

Control Enhancement(s):

(2) *SECURITY AND PRIVACY ARCHITECTURES | SUPPLIER DIVERSITY*

Supplemental C-SCRM Guidance: Supplier diversity provides options for addressing information security and cyber supply chain concerns. The organization should incorporate this control as it relates to suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

The organization should plan for potential replacement of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers in case one is no longer able to meet the organization's requirements (e.g., company goes out of business or does not meet contractual obligations).

Incorporate supplier diversity for off-the-shelf (commercial or government) components during acquisition security assessments. Evaluation of alternatives should include, for example, feature parity, interoperability, commodity components, and ability to provide multiple delivery paths.

Level(s): 2, 3

PL-9 CENTRAL MANAGEMENT

Supplemental C-SCRM Guidance: C-SCRM controls are managed centrally at Level 1 through C-SCRM Strategy & Implementation Plan, and at Levels 1 and 2 through C-SCRM Policy. C-SCRM PMO described in Section 2, centrally manages C-SCRM controls at those two Levels. At Level 3, C-SCRM controls are managed on an information system basis though SSP and/or C-SCRM Plan.

Level(s): 1, 2

PL-10 BASELINE SELECTION

Supplemental C-SCRM Guidance: Organizations should include C-SCRM controls in their control baselines. Organizations should identify and select C-SCRM controls based on C-SCRM requirements identified within each of the levels. A C-SCRM PMO may assist in identifying C-SCRM control baselines that meet common C-SCRM requirements for different groups, communities of interest, or the organization as a whole.

Level(s): 1, 2

FAMILY: PROGRAM MANAGEMENT

FIPS 200 does not specify Program Management minimum security requirements.

NIST SP 800-53 Rev. 5 states that "the program management controls … are implemented at the organization level and not directed at individual information systems." Those controls apply to the entire organization (i.e., federal agency) and support the organization's overarching information security program. Program management controls support and provide inputs and feedback to organization-wide C-SCRM activities.

All Program Management controls should be applied in a C-SCRM context. Within federal agencies the C-SCRM PMO function or a similar is responsible for implementing Program Management controls. Section 3 provides guidance on C-SCRM PMO and its functions and responsibilities.

PM-2 INFORMATION SECURITY PROGRAM LEADERSHIP ROLE

Supplemental C-SCRM Guidance: Senior information security officer (e.g., CISO) and senior agency official responsible for acquisition (e.g., Chief Acquisition Officer (CAO) or Senior Procurement Executive (SPE)) have key responsibilities for C-SCRM and the overall cross-organizational coordination and collaboration with other applicable senior personnel within the organization such as the CIO, the head of facilities/physical security, and the risk executive (function). This coordination should occur regardless of specific department and agency organizational structure and specific titles of relevant senior personnel. The coordination could be executed by C-SCRM PMO or another similar function. Section 2 provides more guidance on C-SCRM roles and responsibilities.

Level(s): 1, 2

PM-3 INFORMATION SECURITY AND PRIVACY RESOURCES

Supplemental C-SCRM Guidance: An organization's C-SCRM program- requires dedicated, sustained funding and human resources to successfully implement agency C-SCRM requirements. Section 3 of this document provides guidance on dedicated funding for C-SCRM programs. The organization should also ensure that C-SCRM requirements are integrated into major IT investments to ensure that the funding is appropriately allocated through the capital planning and investment request process. For example, should an RFID infrastructure be required to improve C-SCRM to secure and improve inventory or logistics management efficiency of the organization's supply chain, appropriate IT investments are likely required to ensure successful planning and implementation. Other examples include any investment into the development or test environment for critical components. In such a case, funding and resources are needed to acquire and maintain appropriate information systems, networks, and components to meet specific C-SCRM requirements that support the mission.

Level(s): 1, 2

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

Supplemental C-SCRM Guidance: C-SCRM items should be included in the POA&M at all levels.

Level(s): 2, 3

Related Controls: CA-5, PM-30

PM-5 SYSTEM INVENTORY

Supplemental C-SCRM Guidance: Having a current system inventory is foundational for C-SCRM. Not having a system inventory may lead to organization's inability to identify system and supplier criticality which will result in inability to conduct C-SCRM activities. To ensure that all applicable suppliers are identified and categorized for criticality, organizations should include relevant supplier information in the system inventory and maintain its currency and accuracy.

Level(s): 2, 3

PM-6 MEASURES OF PERFORMANCE

Supplemental C-SCRM Guidance: Organizations should use measures of performance to track implementation, efficiency, effectiveness, and impact of C-SCRM activities. C-SCRM PMO is responsible for creating C-SCRM measures of performance in collaboration with other applicable stakeholders to include identifying appropriate audience and decision makers and providing guidance on data collection, analysis, and reporting.

Level(s): 1, 2

PM-7 ENTERPRISE ARCHITECTURE

Supplemental C-SCRM Guidance: C-SCRM should be integrated when designing and maintaining enterprise architecture.

Level(s): 1, 2

PM-8 CRITICAL INFRASTRUCTURE PLAN

Supplemental C-SCRM Guidance: C-SCRM should be integrated when developing and maintaining critical infrastructure plan.

Level(s): 1

PM-9 RISK MANAGEMENT STRATEGY

Supplemental C-SCRM Guidance: Risk management strategy should address cyber supply chain risks. Section 2, Appendix C, and Appendix D of this document provide guidance on integrating C-SCRM into Risk Management Strategy.

Level(s): 1

PM-10 AUTHORIZATION PROCESS

Supplemental C-SCRM Guidance: C-SCRM should be integrated when designing and implementing authorization processes.

Level(s): 1, 2

PM-11 MISSION AND BUSINESS PROCESS DEFINITION

Supplemental C-SCRM Guidance: Organization's mission and business processes should address cyber supply chain risks. When addressing mission/business process definitions, the organization should ensure that C-SCRM activities are incorporated into the support processes for achieving mission success. For example, a system supporting a critical mission function that has been designed and implemented for easy removal and replacement should a component fail may require the use of somewhat unreliable hardware components. A C-SCRM activity may need to be defined to ensure that the supplier makes component spare parts readily available if replacement is needed.

Level(s): 1, 2, 3

PM-12 INSIDER THREAT PROGRAM

Supplemental C-SCRM Guidance: An insider threat program should include C-SCRM and be tailored for both federal and non-federal agency individuals who have access to agency systems and networks. This control applies to contractors and subcontractors and should be implemented throughout the SDLC.

Level(s): 1, 2, 3

PM-13 SECURITY AND PRIVACY WORKFORCE

Supplemental C-SCRM Guidance: Security and privacy workforce development and improvement should ensure that relevant C-SCRM topics are integrated into the content and initiatives produced by the program. Section 2 provides information on C-SCRM roles and responsibilities. NIST SP 800-161 can be used as a source of topics and activities to include in the security and privacy workforce program.

Level(s): 1, 2

PM-14 TESTING, TRAINING, AND MONITORING

Supplemental C-SCRM Guidance: Organization's testing, training, and monitoring processes should include C-SCRM activities. C-SCRM PMO can provide guidance and support on how to integrate C-SCRM into testing, training, and monitoring plans.

Level(s): 1, 2

PM-15 SECURITY AND PRIVACY GROUPS AND ASSOCIATIONS

Supplemental C-SCRM Guidance: Contact with security and privacy groups and associations should include C-SCRM practitioners and those with C-SCRM responsibilities. Acquisition, legal, critical infrastructure, and supply chain groups and associations should be incorporated. C-SCRM PMO can help

identify agency personnel who could benefit from participation, specific groups to participate in, and relevant topics.

Level(s): 1, 2

PM-16 THREAT AWARENESS PROGRAM

Supplemental C-SCRM Guidance: Threat awareness program should include threats emanating from the supply chain. When addressing supply chain threat awareness, knowledge should be shared between stakeholders within the boundaries of the organization's information sharing policy. C-SCRM PMO can help identify C-SCRM stakeholders to include in threat information sharing, as well as potential sources of information for supply chain threats.

Level(s): 1, 2

PM-17 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION ON EXTERNAL SYSTEMS

Supplemental C-SCRM Guidance: Policy and procedures for controlled unclassified information (CUI) on external systems should include protecting relevant cyber supply chain information. Conversely, it should include protecting agency information residing in external systems, because such external systems are part of agency supply chain.

Level(s): 2

PM-18 PRIVACY PROGRAM PLAN

Supplemental C-SCRM Guidance: Privacy Program Plan should include C-SCRM. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 1, 2

PM-19 PRIVACY PROGRAM LEADERSHIP ROLE

Supplemental C-SCRM Guidance: Privacy program leadership role should be included is a stakeholder in applicable C-SCRM initiatives and activities.

Level(s): 1

PM-20 DISSEMINATION OF PRIVACY PROGRAM INFORMATION

Supplemental C-SCRM Guidance: Dissemination of privacy program information should be protected from cyber supply chain risks.

Level(s): 1, 2

PM-21 ACCOUNTING OF DISCLOSURES

Supplemental C-SCRM Guidance: Accounting of disclosures should be protected from cyber supply chain risks.

Level(s): 1, 2

PM-22 PERSONALLY IDENTIFIABLE INFORMATION QUALITY MANAGEMENT

Supplemental C-SCRM Guidance: Personally identifiable information (PII) quality management should take into account and manage cyber supply chain risks to this information.

Level(s): 1, 2

PM-23 DATA GOVERNANCE BODY

Supplemental C-SCRM Guidance: Data governance body is a stakeholder in C-SCRM and as such should be included in cross-agency collaboration and information sharing of C-SCRM activities and initiatives (e.g., by participating in inter-agency bodies such as the FASC).

Level(s): 1

PM-25 MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION USED IN TESTING, TRAINING, AND RESEARCH

Supplemental C-SCRM Guidance: Cyber supply chain risks to personally identifiable information should be addressed by minimization policies and procedures described in this control.

Level(s): 2

PM-26 COMPLAINT MANAGEMENT

Supplemental C-SCRM Guidance: Complaint management process and mechanisms should be protected from cyber supply chain risks. Organizations should also integrate C-SCRM security and privacy controls when fielding complaints from vendors or the general public (e.g., departments and agencies fielding inquiries related to exclusions and removals).

Level(s): 2, 3

PM-27 PRIVACY REPORTING

Supplemental C-SCRM Guidance: Privacy reporting process and mechanisms should be protected from cyber supply chain risks.

Level(s): 2, 3

PM-28 RISK FRAMING

Supplemental C-SCRM Guidance: C-SCRM should be included in risk framing. Section 2 and Appendix C provide detail guidance on integrating C-SCRM into risk framing.

Level(s): 1

PM-29 RISK MANAGEMENT PROGRAM LEADERSHIP ROLES

Supplemental C-SCRM Guidance: Risk management program leadership roles should include C-SCRM responsibilities and be included in C-SCRM collaboration across the organization. Section 2 and Appendix C provide detail guidance C-SCRM roles and responsibilities.

Level(s): 1

PM-30 SUPPLY CHAIN RISK MANAGEMENT STRATEGY

Supplemental C-SCRM Guidance: Supply Chain Risk Management Strategy (also known as C-SCRM Strategy) should be complemented with a C-SCRM Implementation Plan that lays out detailed initiatives and activities for the organization with timelines and responsible parties. This implementation plan can be a POA&M or be included in a POA&M. Based on the C-SCRM Strategy and Implementation Plan at Level 1, the organization should select and document common C- SCRM controls that need to address the organization, program, and system-specific needs. These controls should be iteratively integrated the C-SCRM Policy at Levels 1 and 2, and C-SCRM Plan (or SSP if required) at Level 3. See Section 2 and Appendix C for further guidance on risk management.

Level(s): 1, 2

Related Controls: PL-2

PM-31 CONTINUOUS MONITORING STRATEGY

Supplemental C-SCRM Guidance: Continuous monitoring strategy and program should integrate C-SCRM controls at Levels 1, 2, and 3 in accordance with Supply Chain Risk Management Strategy.

Level(s): 1, 2, 3

Related Controls: PM-30

PM-32 PURPOSING

Supplemental C-SCRM Guidance: Extending systems assigned to support specific mission or business functions beyond their initial purpose subjects those systems to unintentional risks to include cyber supply chain risks. Application of this control should include explicit incorporation of cyber supply chain exposures.

Level(s): 2, 3

FAMILY: PERSONNEL SECURITY

FIPS 200 specifies the Personnel Security minimum security requirement as follows:

> *Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.*

Personnel that have access to an organization's cyber supply chain should be covered by the organization's personnel security controls. These personnel include acquisition and contracting professionals, program managers, supply chain and logistics professionals, shipping and receiving staff, information technology professionals, quality professionals, mission and business owners, system owners, and information security engineers. Organizations should also work with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to ensure they apply appropriate personnel security controls to the personnel that interact with the organization's supply chain, as appropriate.

PS-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: At each level, personnel security policy and procedures, and related C-SCRM Strategy/Implementation Plan, C-SCRM Policies, and C-SCRM Plan(s) need to define the roles for the personnel who are engaged in the acquisition, management, and execution of supply chain security activities. These roles also need to state acquirer personnel responsibilities with regards to relationships with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Policies and procedures need to consider the full system development life cycle of systems and the roles and responsibilities needed to address the various supply chain infrastructure activities.

Level 1: Applicable roles include risk executive, CIO, CISO, contracting, logistics, delivery/receiving, acquisition security, and other functions providing supporting supply chain activities.

Level 2: Applicable roles include program executive and individuals (e.g., non-federal employees including contractors) within the acquirer organization responsible for program success (e.g., Program Manager and other individuals).

Level 3: Applicable roles include system engineers or system security engineers throughout the operational system life cycle from requirements definition, development, test, deployment, maintenance, updates, replacements, delivery/receiving, and IT.

Roles for supplier, developer, system integrator, external system service provider, and other ICT/OT-related service provider personnel responsible for the success of the program should be noted in an agreement between acquirer and these parties (e.g., contract).

The organization should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 1, 2, 3

Related Control(s): SA-4

PS-3 PERSONNEL SCREENING

Supplemental C-SCRM Guidance: To mitigate insider threat risks, personnel screening policies and procedures should be extended to any contractor personnel with authorized access to information systems, system components, or information system services. Continuous monitoring activities should be commensurate with the contractor's level of access to sensitive, classified, or regulated information and should be consistent with broader organizational policies. Screening requirements should be incorporated into agreements and flowdown to sub-tier contractors.

Level(s): 2, 3

PS-6 ACCESS AGREEMENTS

Supplemental C-SCRM Guidance: The organization should define and document access agreements for all contractors or other external personnel that may have a need to access the organization's data, systems, or network, whether physically or logically. Access agreements should state the appropriate level and method of access to the information system and supply chain network. Additionally, terms of access should be consistent with the organization's information security policy and may need to specify additional restrictions, such as allowing access during specific timeframes, from specific locations, or by only personnel who have satisfied additional vetting requirements. The organization should deploy audit mechanisms to review, monitor, update, and track access by these parties in accordance with the access agreement. As personnel vary over time, the organization should implement a timely and rigorous personnel security update process for the access agreements.

When information systems and network products and services are provided by an entity within the organization, there may be an existing access agreement in place. When such an agreement does not exist, it should be established.

NOTE: While the audit mechanisms may be implemented in Level 3, the agreement process with required updates should be implemented at Level 2 as a part of program management activities.

The organization should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2, 3

PS-7 EXTERNAL PERSONNEL SECURITY

Supplemental C-SCRM Guidance: Third-party personnel that have access to organization's information systems and networks must meet the same personnel security requirements as organizational personnel. Examples of such third-party personnel can include the system integrator, developer, supplier, or external service provider used for delivery, contractors or service providers that are using the ICT/OT systems, or supplier maintenance personnel brought in to address component technical issues not solvable by the organization or system integrator.

Level(s): 2

FAMILY: PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY

Personally identifiable information processing and transparency is a new control family, developed specifically to address PII processing and transparency concerns.

The organization should keep in mind that some suppliers have comprehensive security and privacy practices and systems that may go above and beyond the organization's requirements. The organizations should work with suppliers to understand the extent of their privacy practices and how they meet the organization's needs.

PT-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: Organizations should ensure that supply chain concerns are included in PII processing and transparency policies and procedures, and related C-SCRM Strategy/Implementation Plan, C-SCRM Policies, and C-SCRM Plan. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies.

The procedures can be established for the security and privacy program in general and individual information systems. These policy and procedures should address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and privacy compliance to support systems/components within information systems or the supply chain.

Policies and procedures need to be in place to ensure contracts state what PII data will be shared, which contractor personnel may have access to the PII, controls protecting PII, and how long it can be kept and what happens to it at the end of a contract.

a. When working with a new supplier, ensure that the agreement includes the most recent set of applicable security requirement.

Contractors need to abide by relevant laws and policies regarding information (PII and other sensitive information)

The organization should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 1, 2, 3

FAMILY: RISK ASSESSMENT

FIPS 200 specifies the Risk Assessment minimum security requirement as follows:

> *Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operating of organizational information systems and the associated processing, storage, or transmission of organizational information.*

NIST SP 800-161 Rev. 1 provides guidance for managing an organization's cyber supply chain risks and expands this control to integrate cyber supply chain risk assessment activities, as described in *Section 2* and *Appendix C*.

RA-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: Risk assessments should be performed at the enterprise, mission/program, and operational levels of the organization. The system-level risk assessment should include both the cyber supply chain infrastructure (e.g., development and testing environments, and delivery systems) and the information system/components traversing the cyber supply chain. System-level risk assessments significantly intersect with the SDLC and should complement the organizations broader RMF activities which take part during the SDLC. A criticality analysis will ensure that mission-critical functions and components are given higher priority due to their impact to the mission, if compromised. The policy should include cyber supply chain-relevant roles applicable to performing and coordinating risk assessments across the organization (see Section 2 for the listing and description of roles). Applicable roles within suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers should be defined.

Level(s): 1, 2, 3

RA-2 SECURITY CATEGORIZATION

Supplemental C-SCRM Guidance: Security categorization is critical to C-SCRM at Levels 1, 2, and 3. In addition to FIPS 199 categorization, for C-SCRM, security categorization should be based on the criticality analysis which is performed as part of the SDLC. See Section 2 and NISTIR 8179 for a detailed description of criticality analysis.

Level(s): 1, 2, 3

Related Controls: RA-9

RA-3 RISK ASSESSMENT

Supplemental C-SCRM Guidance: Risk assessments should include an analysis of criticality, threats, vulnerabilities, likelihood, and impact, as described in detail in Appendix C, *C-SCRM Activities in the Risk Management Process*. Data to be reviewed and collected includes C-SCRM-specific roles, processes, and results of system/component and services acquisitions, implementation, and integration. Risk assessments should be performed at Levels 1, 2, and 3. Risk assessments at higher levels should consist primarily of a synthesis of various risk assessments performed at lower levels and used for understanding the overall impact with the Level (e.g., at the organization or mission/function levels). C-SCRM risk assessments should complement and inform risk assessments which are performed as ongoing activities throughout the SDLC and processes should be appropriately aligned to or integrated into ERM processes and governance.

Level(s): 1, 2, 3

Related Control(s): RA-3(1)

RA-5 VULNERABILITY MONITORING AND SCANNING

Supplemental C-SCRM Guidance: Vulnerability monitoring should cover suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers in the organization's supply chain. This includes employing data collection tools to maintain a continuous state of awareness about potential vulnerability to suppliers as well as the information systems/ system components/ and raw inputs they provide through the cyber supply chain. Vulnerability monitoring activities should take place at all three levels of the organization. Scoping vulnerability monitoring activities requires organizations to consider suppliers as well as their sub-suppliers. Organizations should consider use of the *Impact Analysis Tool for Interdependent Cyber Supply Chain Risks* outlined in NISTIR 8272 to track and maintain visibility into the relevant components within their supply chain.

Level(s): 2, 3

Control Enhancement(s):

(3) *VULNERABILITY MONITORING AND SCANNING | BREADTH AND DEPTH OF COVERAGE*

Supplemental C-SCRM Guidance: Organizations monitoring the cyber supply chain for vulnerabilities should express breadth of monitoring based on the criticality and/or risk profile of the supplier or product/component, and the depth of monitoring based on the level of the supply chain monitoring takes place at (e.g., sub-supplier). Where possible – a component inventory (e.g., hardware, software) may aid organizations in capturing the breadth and depth of the products/components within their cyber supply chain that may need to be monitored and scanned for vulnerabilities.

Level(s): 2, 3

(6) *VULNERABILITY MONITORING AND SCANNING | AUTOMATED TREND ANALYSIS*

Supplemental C-SCRM Guidance: Organizations should track trends, over time, in vulnerability to components within the cyber supply chain. This information may help organizations develop procurement strategies that reduce risk exposure density within the supply chain.

Level(s): 2, 3

RA-7 RISK RESPONSE

Supplemental C-SCRM Guidance: Organizations should integrate cyber supply chain risk response capabilities into the overall organization's response posture, ensuring these responses are aligned to and fall within the boundaries of the organization's tolerance for risk. Risk Response should include consideration of risk response identification, evaluation of alternatives, and risk response decision activities.

Level(s): 1, 2, 3

RA-9 CRITICALITY ANALYSIS

Supplemental C-SCRM Guidance: Organizations should complete a criticality analysis as a prerequisite input to cyber supply chain risk assessment activities. First, organizations complete a criticality analysis as part of the *Frame* step of the C-SCRM Risk Management Process. Then, findings generated in *Assess* step activities (e.g., criticality analysis, threat analysis, vulnerability analysis, and mitigation strategies) update and tailor the criticality analysis. A symbiotic relationship exists between the criticality analysis and other *Assess* step activities in that they inform and enhance one another. For a high-quality criticality analysis – organizations should employ it iteratively throughout the SLDC and concurrently across the 3 levels.

Level(s): 1, 2, 3

RA-10 THREAT HUNTING

Supplemental C-SCRM Guidance: C-SCRM Threat Hunting activities should supplement the organizations internal Threat Hunting activities. As a critical part of the cyber supply chain risk management process – organizations should actively monitor for threats to their cyber supply chain. This requires a collaborative effort between C-SCRM and other cyber defense-oriented functions within the organization. Threat hunting capabilities may also be provided via a shared services organization, especially when an organization lacks the resources to perform threat hunting activities themselves. Typical activities include information sharing with peer organizations and actively consuming threat intelligence feeds that flag potential indicators of increased cyber supply chain risks, such as cyber incidents, mergers and acquisitions, and Foreign Ownership, Control or Influence (FOCI) that may be of concern. Cyber Supply Chain Threat intelligence should seek out threats to the organization's suppliers as well as information systems/ system components/ and raw inputs they provide. Intelligence gathered enables organizations to proactively identify and respond to threats emanating from the supply chain.

Level(s): 1, 2, 3

FAMILY: SYSTEM AND SERVICES ACQUISITION

FIPS 200 specifies the System and Services Acquisition minimum security requirement as follows:

> *Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.*

Organizations acquire ICT/OT products and services through system and services acquisition. These controls address the activities of an acquirer, as well as the activities of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers and related upstream supply chain relationships. They address both physical and logical aspects of cyber supply chain security, from detection to SDLC and security engineering principles. C-SCRM concerns are already prominently addressed in NIST SP 800-53 Rev. 5. NIST SP 800-161 Rev. 1 adds further detail and refinement to these controls.

SA-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: System and services acquisition policy and procedures should address C-SCRM throughout the acquisition management life cycle process, to include purchases made via charge cards. C-SCRM procurement actions and resultant contracts should include requirements language or clauses that address which controls are mandatory or desirable and may include implementation specifications, state what is accepted as evidence that the requirement is satisfied, and how conformance to requirements will be verified and validated. C-SCRM should also be included as an evaluation factor. These applicable procurements should not be limited to only those that are directly related to providing an ICT/OT product or service; while C-SCRM considerations must be applied to these purchases, C-SCRM should also be considered for any and all procurements of products or services in which there may be an unacceptable risk of a supplied product or service contractor compromising the integrity, availability, or confidentiality of an organization's information. This initial assessment should occur during the acquisition planning phase and will be minimally informed by an identification and understanding of the criticality of the organization's mission functions, its high value assets, and the sensitivity of the information that may be accessible by the supplied product or service provider. In addition, organizations should develop policies and procedures that address supply chain risks that may arise during contract performance, such as a change of ownership or control of the business or when actionable information is learned that indicates a supplier or a product is a target of a supply chain threat. Supply chains evolve continuously through mergers and acquisitions, joint ventures, and other partnership agreements. The policy should help organizations understand these changes and use thus obtained information to inform their C-SCRM activities. Organizations can obtain status of such changes through, for example, monitoring public announcements about company activities or any communications initiated by suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. See Section 3 for further guidance on C-SCRM in the federal acquisition process.

Level(s): 1, 2, 3

SA-2 ALLOCATION OF RESOURCES

Supplemental C-SCRM Guidance: The organization should incorporate C-SCRM requirements when determining and establishing the allocation of resources.

Level(s): 1, 2

SA-3 SYSTEM DEVELOPMENT LIFE CYCLE

Supplemental C-SCRM Guidance: There is a strong relationship between the SDLC and C-SCRM activities. The organization should ensure that C-SCRM activities integrated into the SDLC for both the organization and for applicable suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. In addition to traditional SDLC activities, such as requirements and design, the SDLC includes activities such as inventory management, acquisition and procurement, and logical delivery of systems and components. See *Section 2* and *Appendix C* for further guidance on SDLC.

Level(s): 1, 2, 3

SA-4 ACQUISITION PROCESS

Supplemental C-SCRM Guidance: Organizations are to include C-SCRM requirements, descriptions, and criteria in applicable contractual agreements.

a. Organizations are to establish baseline and tailor-able C-SCRM requirements to apply and incorporate into contractual agreements when procuring a product or service from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers; These include but are not limited to:
    1. C-SCRM requirements that cover regulatory mandates (e.g. prohibition of certain ICT/OT or suppliers; address identified and selected controls that are applicable to reducing cyber-supply chain risk that may be introduced by a procured product or service; and provide assurance that the contractor is sufficiently responsible, capable, and trustworthy.
    2. Requirements for critical elements in the supply chain to demonstrate a capability to remediate emerging vulnerabilities based on open source information and other sources;
    3. Requirements for managing intellectual property ownership and responsibilities for elements such as software code, data and information, the manufacturing/development/integration environment, designs, and proprietary processes when provided to the organization for review or use;
    4. Requirements that address the expected life span of the product or system and any element(s) which may be in a critical path based on their life span, as well as what is required when end-of-life is near or has been reached. Organizations should conduct research or solicit information from bidders or existing providers under contract to understand what end-of-life options exist (i.e., replace, upgrade, migrate to a new system, etc.).
    5. Articulate any circumstances when secondary market components may be permitted.

b. Requirements for functional properties, configuration, and implementation information, as well as any development methods, techniques, or practices which may be relevant; Identify and specify C-SCRM evaluation criteria, to include weighting of such criteria

c. Organizations should:
    1. Establish a plan for acquisition of spare parts to ensure adequate supply and execute the plan, if/when applicable;
    2. Establish a plan for acquisition of alternative sources of supply, as may be necessary during continuity events or if/when a disruption to the supply chain occurs,

d. Work with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to identify and define existing and acceptable incident response and information sharing processes, including inputs on vulnerabilities from other organizations within their supply chains;

e. Establish and maintain verification procedures and acceptance criteria for delivered products and services;

f. Ensure that the continuous monitoring plan includes supply chain aspects in its criteria such as. including the monitoring of functions/ports/protocols in use. See Section 2 and Appendix C;
g. Ensure the contract addresses the monitoring of suppliers', developers', system integrators', external system service providers', and other ICT/OT-related service providers' information systems located within the supply chain infrastructure. Monitor and evaluate the acquired work processes and work products where applicable;
h. Communicate processes for reporting information security weaknesses and vulnerabilities detected during the use of ICT/OT products or services and ensure reporting to appropriate stakeholders, including OEMs where relevant;
i. Review and confirm sustained compliance s with the terms and conditions of the agreement on an ongoing basis; and

Level(s): 1, 2, 3

Related Controls: SA-4 (1), (2), (3), (6) and (7)

Control Enhancement(s):

(5) *ACQUISITION PROCESS | SYSTEM, COMPONENT, AND SERVICE CONFIGURATIONS*

Supplemental C-SCRM Guidance: If an organization needs to purchase components, they need to ensure that the product specifications are "fit for purpose" and meet the organization's requirements, whether purchasing directly from the OEM, channel partners, or secondary market.

Level(s): 3

(7) *ACQUISITION PROCESS | NIAP-APPROVED PROTECTION PROFILES*

Supplemental C-SCRM Guidance: This control enhancement requires that the organization build, procure, and/or use U.S. government protection profile-certified information assurance (IA) components when possible. NIAP certification can be achieved for OTS (COTS and GOTS).

Level(s): 2, 3

(8) *ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN FOR CONTROLS*

Supplemental C-SCRM Guidance: This control enhancement is relevant to C-SCRM and plans for continuous monitoring of control effectiveness and should therefore be extended to suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

Level(s): 2, 3

SA-5 SYSTEM DOCUMENTATION

Supplemental C-SCRM Guidance: Information system documentation should include relevant C- SCRM concerns (e.g., C-SCRM plan).

Level(s): 3

SA-8 SECURITY AND PRIVACY ENGINEERING PRINCIPLES

Supplemental C-SCRM Guidance: The following security engineering techniques are helpful in managing cyber supply chain risks:

a. Anticipate the maximum possible ways that the ICT/OT product or service can be misused and abused in order to help identify how to protect the product or system from such uses. Address intended and unintended use scenarios in architecture and design;
b. Design network and security architectures, systems and components based on the organization's risk tolerance as determined by risk assessments (see Section 2 and Appendix C);
c. Document and gain management acceptance and approval for risks that are not fully mitigated;
d. Limit the number, size, and privilege levels of critical elements; using criticality analysis will aid in determining which elements or functions are critical. See criticality analysis in Appendix C, and NISTIR 8179 *Criticality Analysis Process Model: Prioritizing Systems and Components*;
e. Use security mechanisms that help to reduce opportunities to exploit supply chain vulnerabilities, including, for example, encryption, access control, identity management, and malware or tampering discovery;
f. Design information system components and elements to be difficult to disable (e.g., tamper-proofing techniques) and, if disabled, trigger notification methods such as audit trails, tamper evidence, or alarms;
g. Design delivery mechanisms (e.g., downloads for software) to avoid unnecessary exposure or access to the cyber supply chain and the systems/components traversing the cyber supply chain during delivery; and
h. Design relevant validation mechanisms to be used during implementation and operation.

Level(s): 1, 2, 3

SA-9 EXTERNAL SYSTEM SERVICES

Supplemental C-SCRM Guidance: C-SCRM supplemental guidance is provided in control enhancements.

Control Enhancement(s):

(1) *EXTERNAL SYSTEM SERVICES | RISK ASSESSMENTS AND ORGANIZATIONAL APPROVALS*

Supplemental C-SCRM Guidance: See Appendix C - Assess, and Appendices D and E.

Level(s): 2, 3

(3) *EXTERNAL SYSTEM SERVICES | ESTABLISH AND MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS*

Supplemental C-SCRM Guidance: Relationships with providers ("providers" within the context of this enhancement may include suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers) should meet the following supply chain security requirements:
a. Requirements definition is complete and reviewed for accuracy and completeness including the assignment of criticality to various components as well as defining operational concepts and associated scenarios for intended and unintended use in requirements;
b. Requirements are based on needs, relevant compliance drivers, criticality analysis, and cyber supply chain risk assessment;
c. Cyber-supply chain threats, vulnerabilities, and associated risks are identified and documented;
d. Organizational data and information integrity, confidentiality, and availability requirements are defined and shared with the system suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers as appropriate;
e. Consequences of noncompliance with C-SCRM requirements and information system security requirements are defined and documented;
f. Clear delineation of accountabilities, roles, and responsibilities between contractors when multiple disparate providers are engaged in supporting a system or mission/business function.
g. Requirements for service contract completion and what defines the end of the suppliers', developers', system integrators', external system service providers', or other ICT/OT-related

service providers' relationship. This is important to know for re-compete, potential change in provider, and to manage system end-of-life processes.

Level(s): 1, 2, 3

(4) *EXTERNAL SYSTEM SERVICES | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS*

Supplemental C-SCRM Guidance: "Providers" in the context of this enhancement may include suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

Level(s): 3

(5) *EXTERNAL SYSTEM SERVICES | PROCESSING, STORAGE, AND SERVICE LOCATION*

Supplemental C-SCRM Guidance: Location may be under the control of the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Organizations should assess C-SCRM risks associated with a given geographic location and apply an appropriate risk response, which may include defining locations that are or are not acceptable and ensuring appropriate protections are in place to address any associated C-SCRM risks.

Level(s): 3

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Supplemental C-SCRM Guidance: Developer configuration management is critical for reducing cyber supply chain risks. By conducting configuration management activities, developers reduce occurrence and likelihood of flaws, while increasing accountability and ownership for the changes. Developer configuration management should be performed both by developers internal to federal agencies and integrators or external service providers.

Level(s): 2, 3

Related Controls: SA-10 (1), (2), (3), (4), (5), and (6)

SA-11 DEVELOPER TESTING AND EVALUATION

Supplemental C-SCRM Guidance: Depending on the origins of components, this control may be implemented differently. For OTS (off-the-shelf) components, the acquirer should conduct research (e.g., via publicly available resources) or request proof to determine whether the supplier (OEM) has performed such testing as part of their quality/security processes. When the acquirer has control over the application and the development processes, they should require this testing as part of the SDLC. In addition to the specific types of testing activities described in the enhancements, examples of C-SCRM-relevant testing include testing for counterfeits, verifying the origins of components, examining configuration settings prior to integration, and testing interfaces. These types of tests may require significant resources and should be prioritized based on criticality, threat, and vulnerability analyses (described in Section 2 and Appendix C), and the effectiveness of testing techniques. Organizations may also require third-party testing as part of developer security testing.

Level(s): 1, 2, 3

Related Controls: SA-11 (1), (2), (3), (4), (5), (6), (7), (8), and (9)

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Supplemental C-SCRM Guidance: Providing documented and formalized development processes to guide internal and system integrator developers is critical to organizations efforts to effectively mitigate cyber supply chain risks. The organization should apply national and international standards and best practices when implementing this control. Using existing standards promotes consistency of implementation, reliable and defendable process, if implemented properly, and interoperability. The organization's development/maintenance, test, and deployment environments should all be covered by this control. The tools included in this control can be manual or automated. Use of automated tools aids thoroughness, efficiency, and scale of analysis that helps address cyber supply chain risks in the development process. Additionally, the output of such activities and tools provides useful inputs for C-SCRM processes described in Section 2 and Appendix C. This control has applicability to both the internal organization's processes, information systems, and networks as well as applicable system integrators' processes, systems, and networks.

Level(s): 2, 3

Related Controls: SA-15 enhancements (1), (2), (5), (6), and (7)

Control Enhancement(s):

(3) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CRITICALITY ANALYSIS*

Supplemental C-SCRM Guidance: This enhancement identifies critical components within the information system. Doing so will help determine the specific C-SCRM activities to be implemented for critical components. See C-SCRM Criticality Analysis described in Appendix C for additional context.

Level(s): 2, 3

(4) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | THREAT MODELING AND VULNERABILITY ANALYSIS*

Supplemental C-SCRM Guidance: This enhancement provides threat modeling/vulnerability analysis for the relevant federal agency and contractor information systems and networks. Performing this analysis will help integrate C-SCRM into code refinement and modification activities. See C-SCRM threat and vulnerability analyses described in Appendix C for additional context.

Level(s): 2, 3

Related Control(s): SA-15(5), SA-15(6), SA-15(7)

(8) *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | REUSE OF THREAT AND VULNERABILITY INFORMATION*

Supplemental C-SCRM Guidance: This enhancement encourages developers to reuse threat and vulnerability information produced by prior development efforts and lessons learned from using the tools to inform ongoing development efforts. Doing so will help determine C-SCRM activities described in Section 2 and Appendix C.

Level(s): 3

SA-16 DEVELOPER-PROVIDED TRAINING

Supplemental C-SCRM Guidance: Developer-provided training for external and internal (in-house) developers is critical to C-SCRM. It addresses training the individuals responsible for federal systems and networks to include applicable development environments. Developer-provided training in this control also

applies to the individuals who select system and network components. Developer-provided training should include C-SCRM material to ensure that 1) developers are aware of potential threats and vulnerabilities when developing, testing, and maintaining hardware and software; and 2) individuals responsible for selecting system and network components incorporate C-SCRM when choosing such components.

Level(s): 2, 3

Related Controls: AT-3

SA-17 DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN

Supplemental C-SCRM Guidance: This control facilitates the use of C-SCRM information to influence system architecture, design, and component selection decisions, including security functions. Examples include identifying components that compose system architecture and design or selecting specific components to ensure availability through multiple supplier or component selections.

Level(s): 2, 3

Related Controls: SA-17 (1) and (2)

SA-20 CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS

Supplemental C-SCRM Guidance: The organization may decide, based on their cyber supply chain risk assessment, that they require customized development of certain critical components. This control provides additional guidance on this activity.

Level(s): 2, 3

SA-21 DEVELOPER SCREENING

Supplemental C-SCRM Guidance: The organization should implement screening processes for their internal developers. For system integrators who may be providing key developers that address critical components, the organization should ensure that appropriate processes for developer screening have been used. Screening of developers should be included as a contractual requirement and be a flow-down requirement to relevant sub-level subcontractors who provide development services or who have access to the development environment.

Level(s): 2, 3

Control Enhancement(s):

(1) *DEVELOPER SCREENING | VALIDATION OF SCREENING*

Supplemental C-SCRM Guidance: Internal developer screening should be validated. Organizations may validate system integrator developer screening by requesting summary data from the system integrator to be provided post-validation.

Level(s): 2, 3

SA-22 UNSUPPORTED SYSTEM COMPONENTS

Supplemental C-SCRM Guidance: Acquiring products directly from qualified original equipment manufacturers (OEMs) or their authorized distributors and resellers significantly reduces many cyber supply chain risks. In the case of unsupported system components, the organization should use authorized distributors with an ongoing relationship with the supplier of the unsupported system components.

5058
5059 When purchasing alternate sources for continued support, organizations should acquire directly from vetted
5060 original equipment manufacturers (OEMs) or their authorized distributors and resellers. Decisions about
5061 using alternate sources require input from the organization's engineering resources regarding the
5062 differences in alternate component options. For example, if an alternative is to acquire an open source
5063 software component, what are the open source community development, test, acceptance, and release
5064 processes?
5065
5066 Level(s): 2, 3
5067
5068

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

FIPS 200 specifies the System and Communications Protection minimum security requirement as follows:

> *Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.*

An organization's communications infrastructure is composed of ICT/OT components and systems, which have their own supply chains. These communications allow users or administrators to remotely access an organization's systems and to connect to the Internet, with other ICT/OT within the organization, contractor systems, and occasionally supplier systems. An organization's communications infrastructure may be provided and supported by suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

SC-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: System and communications protection policies and procedures should address cyber supply chain risks to the organization's processes, systems, and networks. Organization-level and program-specific policies help establish and clarify these requirements and corresponding procedures provide instructions for meeting these requirements. Policies and procedures should include the coordination of communications among and across multiple organizational entities within the organization as well as communications methods, external connections, and processes used between the organization and its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

Level(s): 1, 2, 3

SC-4 INFORMATION IN SHARED RESOURCES

Supplemental C-SCRM Guidance: The organization may share information system resources with system suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Protecting information in shared resources in support of various supply chain activities is challenging when outsourcing key operations. Organizations may either share too much, increasing their risk, or share too little, making it difficult for the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to be efficient in their service delivery. The organization should work with developers to define a structure/process of information sharing including the data shared, method of sharing, and to whom (the specific roles) it is provided. Appropriate privacy, dissemination, handling, and clearance requirements should be accounted for in the information sharing process.

Level(s): 2, 3

SC-5 DENIAL-OF-SERVICE PROTECTION

Supplemental C-SCRM Guidance: C-SCRM Guidance supplemental guidance is provided in control enhancement SC-5 (2).

Control Enhancement(s):

(2) *DENIAL-OF-SERVICE PROTECTION | CAPACITY, BANDWIDTH, AND REDUNDANCY*

Supplemental C-SCRM Guidance: The organization should include requirements for excess capacity, bandwidth, and redundancy into agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

Level(s): 2

SC-7 BOUNDARY PROTECTION

Supplemental C-SCRM Guidance: The organization should implement appropriate monitoring mechanisms and processes at the boundaries between the agency systems and suppliers', developers', system integrators', external system service providers', and other ICT/OT-related service providers' systems. Provisions for boundary protections should be incorporated into agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. There may be multiple interfaces throughout the organization's and supplier systems and networks and the SDLC. Appropriate vulnerability, threat, and risk assessments should be performed to ensure proper boundary protections for both supply chain components as well as supply chain information flow. The vulnerability, threat, and risk assessment can aid in scoping boundary protection to a relevant set of criteria and help manage associated costs. For contracts with external service providers, organizations should ensure that the provider satisfies boundary control requirements pertinent to environments and networks within their span of control. Further detail is provided in Section 2 and Appendix C.

Level(s): 2

Control Enhancement(s):

(13) *BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS*

Supplemental C-SCRM Guidance: The organization should provide separation and isolation of development, test, and security assessment tools, and operational environments and relevant monitoring tools within the organization's information systems and networks. This control applies the entity responsible for creating software and hardware, to include federal agencies and prime contractors. As such this controls applies to the federal agency and applicable supplier information systems and networks. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. If a compromise or information leakage happens in any one environment, the other environments should still be protected through the separation/isolation mechanisms or techniques.

Level(s): 3

Related Controls: SR-3(3)

(14) *BOUNDARY PROTECTION | PROTECT AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS*

Supplemental C-SCRM Guidance: This control is relevant to C-SCRM as it applies to external service providers.

Level(s): 2,3

Related Controls: SR-3(3)

(19) *BOUNDARY PROTECTION | BLOCKS COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS*

Supplemental C-SCRM Guidance: This control is relevant to C-SCRM as it applies to external service providers.

Level(s): 3

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Supplemental C-SCRM Guidance: Requirements for transmission confidentiality and integrity should be integrated into agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Acquirers, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers may repurpose existing security mechanisms (e.g., authentication, authorization, or encryption) to achieve organizational confidentiality and integrity requirements. The degree of protection should be based on the sensitivity of information to be transmitted and the relationship between the organization and the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

Level(s): 2, 3

SC-18 MOBILE CODE

Supplemental C-SCRM Guidance: The organization should use this control in various applications of mobile code within their information systems and networks. Examples include acquisition processes such as electronic transmission of supply chain information (e.g., email), receipt of software components, logistics information management in RFID, or transport sensors infrastructure.

Level(s): 3

Control Enhancement(s):

(2) *MOBILE CODE | ACQUISITION, DEVELOPMENT, AND USE*

Supplemental C-SCRM Guidance: The organization should employ rigorous supply chain protection techniques in the acquisition, development, and use of mobile code to be deployed in the information system. Examples include ensuring that mobile code originates from vetted sources when acquired, that vetted system integrators are used for the development of custom mobile code or prior to installing, and that verification processes are in place for acceptance criteria prior to install in order to verify the source and integrity of code. Note that mobile code can be both code for the underlying information systems and networks (e.g., RFID device applications) or for information systems/components.

Level(s): 3

SC-27 PLATFORM-INDEPENDENT APPLICATIONS

Supplemental C-SCRM Guidance: The use of trusted platform-independent applications is essential to C-SCRM. Platform-independent applications' enhanced portability enables organizations to more readily switch external service providers in the event that one is compromised, thereby reducing vendor dependency cyber supply chain risks. This is especially relevant for critical applications that may be relied on by multiple systems.

Level(s): 2, 3

SC-28 PROTECTION OF INFORMATION AT REST

Supplemental C-SCRM Guidance: The organization should include provisions for protection of information at rest into their agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The organization should also ensure that they provide appropriate protections within the information systems and networks for data at rest for the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers information, such as source code, testing data, blueprints, and intellectual property information. This control should be applied throughout the SDLC including during requirements, development, manufacturing, test, inventory management, maintenance, and disposal. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2, 3

Related Controls: SR-3(3)

SC-29 HETEROGENEITY

Supplemental C-SCRM Guidance: Heterogeneity techniques include use of different operating systems, virtualization techniques, and multiple sources of supply. Multiple sources of supply can improve component availability and reduce the impact of a cyber supply chain compromise. In case of a cyber supply chain compromise, an alternative source of supply will allow the organizations to more rapidly switch to an alternative system/component which may not be affected by the compromise. Also, heterogeneous components decrease the attack surface by limiting the impact to the subset of the infrastructure that is using vulnerable components.

Level(s): 2, 3

SC-30 CONCEALMENT AND MISDIRECTION

Supplemental C-SCRM Guidance: Concealment and misdirection techniques for C-SCRM include the establishment of random resupply times, concealment of location, random change of fake location used, and random change/shifting of information storage into alternate servers/storage mechanisms.

Level(s): 2, 3

Control Enhancement(s):

(2) *CONCEALMENT AND MISDIRECTION | RANDOMNESS*

Supplemental C-SCRM Guidance: Supply chain processes are necessarily structured with predictable, measurable, and repeatable processes for the purpose of efficiency and cost reduction. This opens up the opportunity for potential breach. In order to protect against compromise, the organization should employ techniques to introduce randomness into organizational operations and assets in the organization's systems or networks (e.g., randomly switching among several delivery organizations or routes, or changing the time and date of receiving supplier software updates if previously predictably scheduled).

Level(s): 2, 3

(3) *CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING AND STORAGE LOCATIONS*

Supplemental C-SCRM Guidance: Changes in processing or storage locations can be used to protect downloads, deliveries, or associated supply chain metadata. The organization may leverage such techniques within the organizations' information systems and networks to create uncertainty into the

activities targeted by adversaries. Establishing a few process changes and randomizing the use of them, whether it is for receiving, acceptance testing, storage, or other supply chain activities, can aid in reducing the likelihood of a supply chain event.

Level(s): 2, 3

(4) *CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION*

Supplemental C-SCRM Guidance: The organization can convey misleading information as part of concealment and misdirection efforts to protect the information system being developed and the organization's systems and networks. Examples of such efforts in security include honeynets or virtualized environments. Implementations can be leveraged in conveying misleading information. These may be considered advanced techniques requiring experienced resources to effectively implement them.

Level(s): 2, 3

(5) *CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS*

Supplemental C-SCRM Guidance: The organization may employ various concealment and misdirection techniques to protect information about the information system being developed and the organization's information systems and networks. For example, delivery of critical components to a central or trusted third-party depot can be used to conceal or misdirect any information regarding the component use or the organization using the component. Separating components from their associated information into differing physical and electronic delivery channels and obfuscating the information through various techniques can be used to conceal information and reduce the opportunity for potential loss of confidentiality of the component or its use, condition, and other attributes.

Level(s): 2, 3

SC-36 DISTRIBUTED PROCESSING AND STORAGE

Supplemental C-SCRM Guidance: Processing and storage can be distributed both across the organization's systems and networks and across the SDLC. The organization should ensure that these techniques are applied in both contexts. The following activities can use distributed processing and storage: development, manufacturing, configuration management, test, maintenance, and operations. This control applies to the entity responsible for processing and storage functions or related infrastructure, to include federal agencies and contractors. As such this controls applies to the federal agency and applicable supplier information systems and networks. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2, 3

Related Controls: SR-3(3)

SC-37 OUT-OF-BAND CHANNELS

Supplemental C-SCRM Guidance: C-SCRM-specific supplemental guidance is provided in control enhancement SC-37 (1).

Control Enhancement(s):

(1) *OUT-OF-BAND CHANNELS | ENSURE DELIVERY AND TRANSMISSION*

Supplemental C-SCRM Guidance: The organization should employ security safeguards to ensure that only specific individuals or information systems receive the information about the information system

or its development environment and processes. For example, proper credentialing and authorization documents should be requested and verified prior to the release of critical components such as custom chips, custom software, or information during delivery.

Level(s): 2, 3

SC-38 OPERATIONS SECURITY

Supplemental C-SCRM Guidance: The organization should ensure that appropriate supply chain threat and vulnerability information is obtained from and provided to the applicable operational security processes.

Level(s): 2, 3

Related Control(s): SR-7

SC-47 ALTERNATE COMMUNICATIONS PATHS

Supplemental C-SCRM Guidance: If necessary and appropriate, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers should be included in the alternate communication paths described in this control.

Level(s): 1, 2, 3

FAMILY: SYSTEM AND INFORMATION INTEGRITY

FIPS 200 specifies the System and Information Integrity minimum security requirement as follows:

> *Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.*

System and information integrity for systems and components traversing the supply chain is critical for managing cyber supply chain risks. Insertion of malicious code and counterfeits are two primary examples of cyber supply chain risks, both of which can at least partially be addressed by deploying system and information integrity controls. Organizations should ensure that adequate system and information integrity protections are part of C-SCRM.

SI-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: The organization should include C-SCRM in system and information integrity policy and procedures, including ensuring that program-specific requirements for employing various integrity verification tools and techniques are clearly defined. System and information integrity for information systems and components and the underlying information systems and networks is critical for managing cyber supply chain risks. Insertion of malicious code and counterfeits are two primary examples of cyber supply chain risks, both of which can be at least partially addressed by deploying system and information integrity controls.

Level(s): 1, 2, 3

Related Controls: SR-1, 9, 10, 11

SI-2 FLAW REMEDIATION

Supplemental C-SCRM Guidance: Output of flaw remediation activities provides useful input into ICT/OT SCRM processes described in Section 2 and Appendix C.

Level(s): 2, 3

Control Enhancement(s):

(5) *FLAW REMEDIATION | AUTOMATIC SOFTWARE AND FIRMWARE UPDATES*

Supplemental C-SCRM Guidance: The organization should specify the various software assets within its information systems and networks that require automated updates (both indirect and direct). This specification of assets should be defined from criticality analysis results, which provide information on critical and noncritical functions and components (see Section 2 and Appendix C). A centralized patch management process may be employed for evaluating and managing updates prior to deployment. Those software assets that require direct updates from a supplier should only accept updates originating directly from the OEM unless specifically deployed by the acquirer, such as with a centralized patch management process.

Level(s): 2

SI-3 MALICIOUS CODE PROTECTION

Supplemental C-SCRM Guidance: Because the majority of code operated in federal system is not developed by the federal government, malicious code threat often originates from the supply chain. This controls applies to the federal agency and contractors with code-related responsibilities (e.g., code-development, installing patched, performing system upgrades, etc.) as well as applicable contractor information systems and networks. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2, 3

Related Controls: SA-11; SI-7(15); SI-3(4), (6), (8), and (10); SR-3(3)

SI-4 SYSTEM MONITORING

Supplemental C-SCRM Guidance: This control includes monitoring of vulnerabilities resulting from past cyber supply chain compromises, such as malicious code implanted during software development and set to activate after deployment. System monitoring is frequently performed by external service providers. Service-level agreements with these providers should be structured to appropriately reflect this control.

Level(s): 1, 2, 3

Control Enhancement(s):

(17) *SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS*

Supplemental C-SCRM Guidance: System monitoring information may be correlated with that of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, if appropriate. The results of correlating monitoring information may point to cyber supply chain vulnerabilities that require mitigation or compromises.

Level(s): 2, 3

(19) *SYSTEM MONITORING | RISK FOR INDIVIDUALS*

Supplemental C-SCRM Guidance: Persons identified as being of higher risk may include organizational employees, contractors, and other third parties (e.g., volunteers, visitors) that may have the need or ability to access to an organization's system, network, or system environment. In accordance with policies and procedures and, if relevant, terms of an agreement, and in coordination with appropriate officials, the organization may implement enhanced oversight of these higher-risk individuals.

Level(s): 2, 3

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Supplemental C-SCRM Guidance: The organization should evaluate security alerts, advisories, and directives for cyber supply chain impact and follow up if needed. U.S. Cert, FASC, and other authoritative entities, generate security alerts and advisories that are applicable to C-SCRM. Additional laws and regulations will impact who and how additional advisories are provided. Organizations should ensure their information sharing protocols and processes include sharing alerts, advisories, and directives with relevant parties with whom they have an agreement to deliver products or perform services. Organization's should provide direction or guidance as to what actions are to be taken in response to sharing such an alert, advisory, or directive.

Level(s): 1, 2, 3

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Supplemental C-SCRM Guidance: This control applies to the federal agency and applicable supplier information systems and networks. The integrity of all applicable systems and networks should be systematically tested and verified to ensure that it remains as required so that the systems/components traversing through the supply chain are not impacted by unanticipated changes. The integrity of systems and components should also be tested and verified. Applicable verification tools include: digital signature or checksum verification, acceptance testing for physical components, confining software to limited privilege environments such as sandboxes, code execution in contained environments prior to use, and ensuring that if only binary or machine-executable code is available, it is obtained directly from the OEM or a verified supplier or distributer. Mechanisms for this control are discussed in detail in NIST SP 800-53 Rev. 5. This controls applies to the federal agency and applicable supplier information systems and networks. When purchasing an ICT/OT product, an organization should perform due diligence to understand what a supplier's integrity assurance practices are. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2, 3

Related Controls: SR-3(3)

Control Enhancement(s):

(14) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE*

Supplemental C-SCRM Guidance: The organization should obtain binary or machine-executable code directly from the OEM/developer or other verified source.

Level(s): 2, 3

(15) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION*

Supplemental C-SCRM Guidance: The organization should ensure that code authentication mechanisms such as digital signatures are implemented to assure the integrity of software, firmware, and information.

Level(s): 3

SI-12 INFORMATION MANAGEMENT AND RETENTION

Supplemental C-SCRM Guidance: C-SCRM should be included in information management and retention requirements, especially when system integrator, supplier, and external service provider sensitive and proprietary information is concerned.

Level(s): 3

SI-20 TAINTING

Supplemental C-SCRM Guidance: Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers may have access to federal agency sensitive information. If that is the case, organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

5456 Level(s): 2, 3
5457
5458 Related Controls: SR-9

FAMILY: SUPPLY CHAIN RISK MANAGEMENT

FIPS 200 does not specify Supply Chain Risk Management minimum security requirements. NIST SP 800-53 Rev. 5 established a new control family: Supply Chain Risk Management. Supplemental guidance below expands upon the SR controls and provides further information and context for their application.

SR-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: C-SCRM policies is developed at Level 1 for the overall organization and at Level 2 for specific missions and functions. C-SCRM policies can be implemented at Levels 1, 2, and 3, depending on the level of depth and detail. C-SCRM procedures are developed at Level 2 for specific missions and functions and at Level 3 for specific systems. Organizational functions including but not limited to information security, legal, risk management, and acquisition should review and concur on the development of C-SCRM policies and procedures or providing guidance to system owners for developing system-specific C-SCRM procedures.

Level(s): 1, 2, 3

SR-2 SUPPLY CHAIN RISK MANAGEMENT PLAN

Supplemental C-SCRM Guidance: C-SCRM plans describes implementations, requirements, constraints, and implications at the system level. C-SCRM plans are influenced by the organization's other risk assessment activities and may inherit and tailor common control baselines defined at Level 1 and 2. C-SCRM plans defined at Level 3 works in collaboration with the organization's C-SCRM Strategy and Policies (Levels 1 & 2), and the C-SCRM Implementation Plan (Levels 1 & 2) to provide a systematic and holistic approach for cyber supply chain risk management across the organization.

C-SCRM plans should be developed as a standalone document and only integrated in existing system security plans if organizational constraints require it.

Level(s): 3

Related Controls: PL-2

SR-3 SUPPLY CHAIN CONTROLS AND PROCESSES

Supplemental C-SCRM Guidance: Section 2 and Appendix C of this document provide detailed guidance on implementing this control.

Level(s): 1, 2, 3

Control Enhancement(s):

(1) *SUPPLY CHAIN CONTROLS AND PROCESSES | DIVERSE SUPPLY BASE*

Supplemental C-SCRM Guidance: Organizations should diversify their supply base, especially for critical ICT/OT products and services. As a part of this exercise the organization should attempt to identify single points of failure and risk among primes and lower level entities in the supply chain. Criticality analysis as described in NISTIR 8272, *Impact Analysis Tool for Interdependent Cyber*

Supply Chain Risks can help determine which suppliers are critical. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis.

Level(s): 2, 3

Related Controls: RA-9

(3) *SUPPLY CHAIN CONTROLS AND PROCESSES | SUB-TIER FLOW DOWN*

Supplemental C-SCRM Guidance: Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors throughout the SDLC. The use of the acquisition process provides an important vehicle to protect the supply chain. Organization should include as part of procurement requirements the need for suppliers to flow down controls to subcontractors throughout the SDLC. As part of market research and analysis activities, organization should conduct robust due diligence research on potential suppliers or products as well as their upstream dependencies (i.e., 4th and 5th party suppliers). The results of this research can be helpful in shaping the sourcing approach and refining requirements. Then, during the solicitation and contract award phase, an evaluation of the cyber supply chain risks associated with a supplier, product, or service should be completed prior to the contract award decision to ensure the holistic risk profile is well understood and serves as a weighted factor in award decisions. During the period of performance, suppliers should be monitored for conformance to the defined controls and requirements, as well as changes in risk conditions. See Section 3 for guidance on the Role of C-SCRM in the Acquisition Process.

Level(s): 2, 3

SR-4 PROVENANCE

Supplemental C-SCRM Guidance: Provenance should be applied to systems, system components, and associated data throughout the SDLC.

Level(s): 2, 3

SR-5 ACQUISITION STRATEGIES, TOOLS, AND METHODS

Supplemental C-SCRM Guidance: Section 3 and SA controls provide additional guidance on acquisition strategies, tools, and methods.

Level(s): 1, 2, 3

Related Controls: SA Control Family

SR-6 SUPPLIER ASSESSMENTS AND REVIEWS

Supplemental C-SCRM Guidance: In general, an organization should consider any information pertinent to the security, integrity, resilience, quality, trustworthiness, or authenticity of the supplier, or their provided services or products. Organizations should consider applying this information against a consistent set of core, baseline factors and assessment criteria to facilitate equitable comparison (between suppliers as well as over time). Depending upon the specific context and purpose for which the assessment is being conducting, the organization may select additional factors. The quality of information (e.g., its relevance,

completeness, accuracy, etc.) relied upon for an assessment is also an important consideration. Reference sources for assessment information should also be documented. The C-SCRM PMO can help define requirements, methods, and tools for organization's supplier assessments.

Level(s): 2, 3

SR-7 SUPPLY CHAIN OPERATIONS SECURITY

Supplemental C-SCRM Guidance: C-SCRM PMO can help determine OPSEC controls that apply to specific missions and functions. OPSEC controls are particularly important when there is specific concern about an adversarial threat from or to the organization's supply chain or an element within the supply chain or the nature of the organization's mission or business operations, its information, and/or its service/product offerings may make it a more attractive target of an adversarial threat.

Level(s): 2, 3

SR-8 NOTIFICATION AGREEMENTS

Supplemental C-SCRM Guidance: Organizations should require their suppliers, minimally, have established notification agreements with those entities within their supply chain that have a role or responsibility related to that critical service or product.

Level(s): 2, 3

Related Controls: RA-9

SR-9 TAMPER RESISTANCE AND DETECTION

Supplemental C-SCRM Guidance: Organizations should apply tamper resistance and detection control to critical components, at a minimum. Criticality analysis can help determine which components are critical. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis. C-SCRM PMO can help identify critical components, especially those that are used by multiple missions, functions, and systems within an organization.

Level(s): 2, 3

Related Controls: RA-9

SR-10 INSPECTION OF SYSTEMS OR COMPONENTS

Supplemental C-SCRM Guidance: Organizations should inspect critical systems and components, at a minimum, for assurance that tamper resistance controls are in place and to examine whether there is evidence of tampering. Products or components should be inspected prior to use and periodically thereafter. Inspection requirements should also be included in contracts with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors and flow down to subcontractors, when relevant.

Criticality analysis can help determine which systems and components are critical and should therefore be subjected to inspection. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis. C-SCRM PMO can help identify critical systems and components, especially those that are used by multiple missions, functions, and systems (for components) within an organization.

Level(s): 2, 3

Related Controls: RA-9

SR-11 COMPONENT AUTHENTICITY

Supplemental C-SCRM Guidance: Development of anti-counterfeit policy and procedures requires input from and coordination with acquisition, Information Technology, IT Security, legal, and the C-SCRM PMO. The policy and procedures should address regulatory compliance requirements, contract requirements/clauses as well as counterfeit reporting processes to organizations such as GIDEP and/or other appropriate organizations.

Level(s): 1, 2, 3

Control Enhancement(s):

(1) *COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING*

Supplemental C-SCRM Guidance: C-SCRM PMO can assist in identifying resources that can provide anti-counterfeit training and/or may be able to conduct such training for the organization. The C-SCRM PMO can also assist in identifying which personnel should receive the training.

Level(s): 2, 3

(2) *COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR*

Supplemental C-SCRM Guidance: Information Technology, IT Security, or the C-SCRM PMO should be responsible for establishing and implementing configuration control processes for component service and repair, to include, if applicable, integrating component service and repair into the overall organizational configuration control processes. Component authenticity should be addressed in contracts when procuring component servicing and repair support.

Level(s): 2, 3

(3) *COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT SCANNING*

Supplemental C-SCRM Guidance: Organizations should conduct anti-counterfeit scanning for critical components, at a minimum. Criticality analysis can help determine which components are critical and should be subjected to this scanning. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis. C-SCRM PMO can help identify critical components, especially those that are used by multiple missions, functions, and systems within an organization.

Level(s): 2, 3

Related Controls: RA-9

SR-12 COMPONENT DISPOSAL

Supplemental C-SCRM Guidance: IT Security, in coordination with the C-SCRM PMO, can help establish appropriate component disposal policies, procedures, mechanisms, and techniques.

Level(s): 2, 3

SR-13 SUPPLIER INVENTORY (NEW)

Control:

a. Develop, document, and maintain an accurate and complete inventory of suppliers that present cyber supply chain risk. This inventory should:
    1. Document organization's suppliers;
    2. Identify whether the supplier provides a product and/or service;
    3. For each supplier, indicate which programs, projects, and systems are using supplier products and services
    4. For each supplier, assign criticality level to each supplier organization that aligns to the criticality of the program, project and/or system (or component of system).

b. Review and update supplier inventory [*Assignment: organization-defined frequency*].

Supplemental C-SCRM Guidance: Organizations rely on numerous suppliers to execute their missions and functions. Many suppliers provide products and services in support of multiple missions, functions, programs, projects, and systems. Some suppliers are more critical than others, based on the criticality of missions, functions, programs, projects, systems that their products and services support, as well as the organization's level of dependency on the supplier. Organizations should use criticality analysis to help determine which products and services are critical to determine criticality of suppliers to be documented in the supplier inventory. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis.

Level(s): 2, 3

Related Controls: RA-9

APPENDIX A: C-SCRM CONTROL SUMMARY

This appendix lists the C-SCRM controls in this publication and maps them to their corresponding NIST SP 800-53 Rev. 5 controls as appropriate. Table A-1 indicates those controls that are defined in NIST SP 800-53 Rev. 5 Low baseline requirements and are deemed to be C-SCRM relevant. Some C-SCRM controls were added to this baseline to form the C-SCRM Baseline. Additionally, controls that should flow down from prime contractors to their relevant sub-tier contractors are listed as Flow Down Controls. Given that C-SCRM is an organization-wide activity that requires selection and implementation of controls at the enterprise, mission/business, and operational levels (Levels 1, 2, and 3 of the organization according to NIST SP 800-39), Table A-1 indicates the organizational levels in which the controls should be implemented. The table highlights C-SCRM controls and enhancements not in NIST SP 800-53 Rev. 5 in red, viz., MA-8 and SR-13.

Table A-1: C-SCRM Control Summary

				Levels		
Control Identifier	**Control (or Control Enhancement) Name**	**C-SCRM Baseline**	**Flow Down Control**	**1**	**2**	**3**
AC-1	**Policy and Procedures**	x	x	x	x	x
AC-2	**Account Management**	x			x	x
AC-3	**Access Enforcement**	x			x	x
AC-3(8)	*Access Enforcement | Revocation of Access Authorizations*				x	x
AC-3(9)	*Access Enforcement | Controlled Release*				x	x
AC-4	**Information Flow Enforcement**		x		x	x
AC-4(6)	*Information Flow Enforcement | Metadata*				x	x
AC-4(17)	*Information Flow Enforcement | Domain Authentication*				x	x
AC-4(19)	*Information Flow Enforcement | Validation of Metadata*				x	x
AC-4(21)	*Information Flow Enforcement | Physical or Logical Separation of Information Flows*					x
AC-5	**Separation of Duties**				x	x
(AC-6)	**(Least Privilege)**	(x)	(N/A)			
AC-6(6)	*Least Privilege | Privileged Access by Non-organizational Users*				x	x
AC-17	**Remote Access**	x	x		x	x
AC-17(6)	*Remote Access | Protection of Mechanism Information*				x	x
AC-18	**Wireless Access**	x		x	x	x
AC-19	**Access Control for Mobile Devices**	x			x	x
AC-20	**Use of External Systems**	x	x	x	x	x
AC-20(1)	*Use of External Systems | Limits on Authorized Use*				x	x
AC-20(3)	*Use of External Systems | Non-organizationally Owned Systems — Restricted Use*				x	x
AC-21	**Information Sharing**			x	x	
AC-22	**Publicly Accessible Content**	x			x	x
AC-23	**Data Mining Protection**		x		x	x
AC-24	**Access Control Decisions**		x	x	x	x
AT-1	**Policy and Procedures**	x		x	x	
(AT-2)	**(Literacy Training and Awareness)**	(x)	(N/A)			

AT-2(1)	*Literacy Training and Awareness | Practical Exercises*				x	
AT-2(2)	*Literacy Training and Awareness | Insider Threat*	x	x		x	
AT-2(3)	*Literacy Training and Awareness | Social Engineering and Mining*				x	
AT-2(4)	*Literacy Training and Awareness | Suspicious Communications and Anomalous System Behavior*				x	
AT-2(5)	*Literacy Training and Awareness | Advanced Persistent Threat*				x	
AT-2(6)	*Literacy Training and Awareness | Cyber Threat Environment*				x	
AT-3	**Role-based Training**	x			x	
AT-3(2)	*Role-based Training | Physical Security Controls*				x	
AT-4	**Training Records**	x			x	
AU-1	**Policy and Procedures**	x		x	x	x
AU-2	**Event Logging**	x		x	x	x
AU-3	**Content of Audit Records**	x		x	x	x
AU-6	**Audit Record Review, Analysis, and Reporting**	x			x	x
AU-6(9)	*Audit Record Review, Analysis, and Reporting | Correlation with Information from Nontechnical Sources*					x
AU-10	**Non-repudiation**					x
AU-10(1)	*Non-repudiation | Association of Identities*				x	
AU-10(2)	*Non-repudiation | Validate Binding of Information Producer Identity*				x	x
AU-10(3)	*Non-repudiation | Chain of Custody*				x	x
AU-12	**Audit Record Generation**	x			x	x
AU-13	**Monitoring for Information Disclosure**				x	x
AU-14	**Session Audit**				x	x
AU-16	**Cross-organizational Audit Logging**				x	x
AU-16(2)	*Cross-organizational Audit Logging | Sharing of Audit Information*		x		x	x
CA-1	**Policy and Procedures**	x		x	x	x
CA-2	**Control Assessments**	x			x	x
CA-2(2)	*Control Assessments | Specialized Assessments*					x
CA-2(3)	*Control Assessments | Leveraging Results from External Organizations*					x
CA-3	**Information Exchange**	x	x			x
CA-5	**Plan of Action and Milestones**	x			x	x
CA-6	**Authorization**	x		x	x	x
(CA-7)	**(Continuous Monitoring)**	(x)	(N/A)			
CA-7(3)	*Continuous Monitoring | Trend Analyses*					x
CM-1	**Policy and Procedures**	x		x	x	x
CM-2	**Baseline Configuration**	x			x	x
CM-2(6)	*Baseline Configuration | Development and Test Environments*				x	x
CM-3	**Configuration Change Control**				x	x
CM-3(1)	*Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes*				x	x
CM-3(2)	*Configuration Change Control | Testing, Validation, and Documentation of Changes*				x	x
CM-3(4)	*Configuration Change Control | Security and Privacy Representatives*				x	x

CM-3(8)	*Configuration Change Control | Prevent or Restrict Configuration Changes*				x	x
CM-4	**Impact Analyses**	x				x
CM-4(1)	*Impact Analyses | Separate Test Environments*					x
CM-5	**Access Restrictions for Change**	x			x	x
CM-5(1)	*Access Restrictions for Change | Automated Access Enforcement and Audit Records*					x
CM-5(6)	*Access Restrictions for Change | Limit Library Privileges*					x
CM-6	**Configuration Settings**	x			x	x
CM-6(1)	*Configuration Settings | Automated Management, Application, and Verification*					x
CM-6(2)	*Configuration Settings | Respond to Unauthorized Changes*					x
CM-7	**Least Functionality**	x	x			x
CM-7(1)	*Least Functionality | Periodic Review*				x	x
CM-7(4)	*Least Functionality | Unauthorized Software*				x	x
CM-7(5)	*Least Functionality | Authorized Software*					x
CM-7(6)	*Least Functionality | Confined Environments with Limited Privileges*				x	x
CM-7(7)	*Least Functionality | Code Execution in Protected Environments*					x
CM-7(8)	*Least Functionality | Binary or Machine Executable Code*				x	x
CM-7(9)	*Least Functionality | Prohibiting the Use of Unauthorized Hardware*				x	x
CM-8	**System Component Inventory**	x			x	x
CM-8(1)	*System Component Inventory | Updates During Installation and Removal*					x
CM-8(2)	*System Component Inventory | Automated Maintenance*					x
CM-8(4)	*System Component Inventory | Accountability Information*					x
CM-8(6)	*System Component Inventory | Assessed Configurations and Approved Deviations*					x
CM-8(7)	*System Component Inventory | Centralized Repository*					x
CM-8(8)	*System Component Inventory | Automated Location Tracking*				x	x
CM-8(9)	*System Component Inventory | Assignment of Components to Systems*					x
CM-9	**Configuration Management Plan**		x		x	x
CM-9(1)	*Configuration Management Plan | Assignment of Responsibility*				x	x
CM-10	**Software Usage Restrictions**	x			x	x
CM-10(1)	*Software Usage Restrictions | Open-source Software*				x	x
CM-11	**User-installed Software**	x			x	x
CM-12	**Information Location**				x	x
CM-12(1)	*Information Location | Automated Tools to Support Information Location*				x	x
CM-13	**Data Action Mapping**				x	x
CM-14	**Signed Components**					x
CP-1	**Policy and Procedures**	x		x	x	x
CP-2	**Contingency Plan**	x			x	x
CP-2(1)	*Contingency Plan | Coordinate with Related Plans*				x	x

CP-2(2)	*Contingency Plan | Capacity Planning*				x	x
CP-2(7)	*Contingency Plan | Coordinate with External Service Providers*		x			x
CP-2(8)	*Contingency Plan | Identify Critical Assets*					x
CP-3	**Contingency Training**	x			x	x
CP-3(1)	*Contingency Training | Simulated Events*				x	x
CP-4	**Contingency Plan Testing**	x			x	x
CP-6	**Alternate Storage Site**				x	x
CP-6(1)	*Alternate Storage Site | Separation from Primary Site*				x	x
CP-7	**Alternate Processing Site**				x	x
CP-8	**Telecommunications Services**				x	x
CP-8(3)	*Telecommunications Services | Separation of Primary and Alternate Providers*				x	x
CP-8(4)	*Telecommunications Services | Provider Contingency Plan*				x	x
CP-11	**Alternate Communications Protocols**				x	x
IA-1	**Policy and Procedures**	x		x	x	x
IA-2	**Identification and Authentication (organizational Users)**	x		x	x	x
IA-3	**Device Identification and Authentication**			x	x	x
IA-4	**Identifier Management**	x			x	x
IA-4(6)	*Identifier Management | Cross-organization Management*			x	x	x
IA-5	**Authenticator Management**	x			x	x
IA-5(5)	*Authenticator Management | Change Authenticators Prior to Delivery*					x
IA-5(9)	*Authenticator Management | Federated Credential Management*					x
IA-8	**Identification and Authentication (non-organizational Users)**	x			x	x
IA-9	**Service Identification and Authentication**				x	x
IR-1	**Policy and Procedures**	x	x	x	x	x
IR-2	**Incident Response Training**	x			x	x
(IR-4)	**(Incident Handling)**	(x)	(N/A)			
IR-3	**Incident Response Testing**				x	x
IR-4(6)	*Incident Handling | Insider Threats*			x	x	x
IR-4(7)	*Incident Handling | Insider Threats — Intra-organization Coordination*			x	x	x
IR-4(10)	*Incident Handling | Supply Chain Coordination*		x		x	
IR-4(11)	*Incident Handling | Integrated Incident Response Team*					x
IR-5	**Incident Monitoring**	x			x	x
(IR-6)	**(Incident Reporting)**	(x)	(N/A)			
IR-6(3)	*Incident Reporting | Supply Chain Coordination*		x			x
(IR-7)	**(Incident Response Assistance)**	(x)	(N/A)			
IR-7(2)	*Incident Response Assistance | Coordination with External Providers*		x			x
IR-8	**Incident Response Plan**	x	x		x	x
IR-9	**Information Spillage Response**		x			x
MA-1	**Policy and Procedures**	x	x	x	x	x
(MA-2)	**(Controlled Maintenance)**	(x)	(N/A)			
MA-2(2)	*Controlled Maintenance | Automated Maintenance Activities*					x

MA-3	**Maintenance Tools**				x	x
MA-3(1)	*Maintenance Tools | Inspect Tools*					x
MA-3(2)	*Maintenance Tools | Inspect Media*					x
MA-3(3)	*Maintenance Tools | Prevent Unauthorized Removal*					x
MA-4	**Nonlocal Maintenance**	x	x		x	x
MA-4(3)	*Nonlocal Maintenance | Comparable Security and Sanitization*				x	x
MA-5	**Maintenance Personnel**	x			x	x
MA-5(4)	*Maintenance Personnel | Foreign Nationals*		x		x	x
MA-6	**Timely Maintenance**					x
MA-7	**Field Maintenance**					x
MA-8	**Maintenance Monitoring and Information Sharing**					x
MP-1	**Policy and Procedures**	x		x	x	
MP-4	**Media Storage**		x	x	x	
MP-5	**Media Transport**			x	x	
MP-6	**Media Sanitization**	x	x		x	x
PE-1	**Policy and Procedures**	x		x	x	x
PE-2	**Physical Access Authorizations**	x	x		x	x
PE-2(1)	*Physical Access Authorizations | Access by Position or Role*				x	x
PE-3	**Physical Access Control**	x			x	x
PE-3(1)	*Physical Access Control | System Access*				x	x
PE-3(2)	*Physical Access Control | Facility and Systems*				x	x
PE-3(5)	*Physical Access Control | Tamper Protection*				x	x
PE-6	**Monitoring Physical Access**	x		x	x	x
PE-16	**Delivery and Removal**	x				x
PE-17	**Alternate Work Site**					x
PE-18	**Location of System Components**			x	x	x
PE-20	**Asset Monitoring and Tracking**				x	x
PE-23	**Facility Location**		x		x	x
PL-1	**Policy and Procedures**	x			x	
PL-2	**System Security and Privacy Plans**	x	x			x
PL-4	**Rules of Behavior**	x			x	x
PL-7	**Concept of Operations**					x
PL-8	**Security and Privacy Architectures**				x	x
PL-8(2)	*Security and Privacy Architectures | Supplier Diversity*				x	x
PL-9	**Central Management**			x	x	
PL-10	**Baseline Selection**	x			x	x
PM-2	**Information Security Program Leadership Role**			x	x	
PM-3	**Information Security and Privacy Resources**			x	x	
PM-4	**Plan of Action and Milestones Process**				x	x
PM-5	**System Inventory**				x	x
PM-6	**Measures of Performance**			x	x	
PM-7	**Enterprise Architecture**			x	x	
PM-8	**Critical Infrastructure Plan**			x		
PM-9	**Risk Management Strategy**			x		
PM-10	**Authorization Process**			x	x	
PM-11	**Mission and Business Process Definition**			x	x	x
PM-12	**Insider Threat Program**			x	x	x
PM-13	**Security and Privacy Workforce**			x	x	
PM-14	**Testing, Training, and Monitoring**			x	x	
PM-15	**Security and Privacy Groups and Associations**			x	x	

PM-16	**Threat Awareness Program**			x	x	
PM-17	**Protecting Controlled Unclassified Information on External Systems**				x	
PM-18	**Privacy Program Plan**		x	x	x	
PM-19	**Privacy Program Leadership Role**			x		
PM-20	**Dissemination of Privacy Program Information**			x	x	
PM-21	**Accounting of Disclosures**			x	x	
PM-22	**Personally Identifiable Information Quality Management**			x	x	
PM-23	**Data Governance Body**			x		
PM-25	**Minimization of Personally Identifiable Information Used in Testing, Training, and Research**				x	
PM-26	**Complaint Management**				x	x
PM-27	**Privacy Reporting**				x	x
PM-28	**Risk Framing**			x		
PM-29	**Risk Management Program Leadership Roles**			x		
PM-30	**Supply Chain Risk Management Strategy**			x	x	
PM-31	**Continuous Monitoring Strategy**			x	x	x
PM-32	**Purposing**				x	x
PS-1	**Policy and Procedures**	x	x	x	x	x
PS-3	**Personnel Screening**	x	x		x	x
PS-6	**Access Agreements**	x	x		x	x
PS-7	**External Personnel Security**	x			x	
PT-1	**Policy and Procedures**		x	x	x	x
RA-1	**Policy and Procedures**	x		x	x	x
RA-2	**Security Categorization**	x		x	x	x
RA-3	**Risk Assessment**	x		x	x	x
RA-5	**Vulnerability Monitoring and Scanning**	x			x	x
RA-5(3)	*Vulnerability Monitoring and Scanning | Breadth and Depth of Coverage*				x	x
RA-5(6)	*Vulnerability Monitoring and Scanning | Automated Trend Analyses*				x	x
RA-7	**Risk Response**	x		x	x	x
RA-9	**Criticality Analysis**			x	x	x
RA-10	**Threat Hunting**			x	x	x
SA-1	**Policy and Procedures**	x		x	x	x
SA-2	**Allocation of Resources**	x		x	x	
SA-3	**System Development Life Cycle**	x		x	x	x
SA-4	**Acquisition Process**	x		x	x	x
SA-4(5)	*Acquisition Process | System, Component, and Service Configurations*					x
SA-4(7)	*Acquisition Process | NIAP-approved Protection Profiles*				x	x
SA-4(8)	*Acquisition Process | Continuous Monitoring Plan for Controls*				x	x
SA-5	**System Documentation**	x				x
SA-8	**Security and Privacy Engineering Principles**	x		x	x	x
(SA-9)	**(External System Services)**	(x)	(N/A)			
SA-9(1)	*External System Services | Risk Assessments and Organizational Approvals*				x	x
SA-9(3)	*External System Services | Establish and Maintain Trust Relationship with Providers*			x	x	x

SA-9(4)	*External System Services | Consistent Interests of Consumers and Providers*					x
SA-9(5)	*External System Services | Processing, Storage, and Service Location*					x
SA-10	**Developer Configuration Management**				x	x
SA-11	**Developer Testing and Evaluation**			x	x	x
SA-15	**Development Process, Standards, and Tools**				x	x
SA-15(3)	*Development Process, Standards, and Tools | Criticality Analysis*				x	x
SA-15(4)	*Development Process, Standards, and Tools | Threat Modeling and Vulnerability Analysis*				x	x
SA-15(8)	*Development Process, Standards, and Tools | Reuse of Threat and Vulnerability Information*					x
SA-16	**Developer-provided Training**				x	x
SA-17	**Developer Security and Privacy Architecture and Design**				x	x
SA-20	**Customized Development of Critical Components**				x	x
SA-21	**Developer Screening**		x		x	x
SA-21(1)	*Developer Screening | Validation of Screening*				x	x
SA-22	**Unsupported System Components**	x			x	x
SC-1	**Policy and Procedures**	x		x	x	x
SC-4	**Information in Shared System Resources**				x	x
(SC-5)	**(Denial-of-service Protection)**	(x)	(N/A)			
SC-5(2)	*Denial-of-service Protection | Capacity, Bandwidth, and Redundancy*				x	
SC-7	**Boundary Protection**	x			x	
SC-7(13)	*Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components*		x			x
SC-7(14)	*Boundary Protection | Protect Against Unauthorized Physical Connections*				x	x
SC-7(19)	*Boundary Protection | Block Communication from Non-organizationally Configured Hosts*					x
SC-8	**Transmission Confidentiality and Integrity**				x	x
SC-18	**Mobile Code**					x
SC-18(2)	*Mobile Code | Acquisition, Development, and Use*					x
SC-27	**Platform-independent Applications**				x	x
SC-28	**Protection of Information at Rest**		x		x	x
SC-29	**Heterogeneity**				x	x
SC-30	**Concealment and Misdirection**				x	x
SC-30(2)	*Concealment and Misdirection | Randomness*				x	x
SC-30(3)	*Concealment and Misdirection | Change Processing and Storage Locations*				x	x
SC-30(4)	*Concealment and Misdirection | Misleading Information*				x	x
SC-30(5)	*Concealment and Misdirection | Concealment of System Components*				x	x
SC-36	**Distributed Processing and Storage**		x		x	x
(SC-37)	**(Out-of-band Channels)**	(x)	(N/A)			x
SC-37(1)	*Out-of-band Channels | Ensure Delivery and Transmission*				x	x
SC-38	**Operations Security**				x	x
SC-47	**Alternate Communications Paths**			x	x	x

SI-1	**Policy and Procedures**	x		x	x	x
SI-2	**Flaw Remediation**	x			x	x
SI-2(5)	*Flaw Remediation | Automatic Software and Firmware Updates*				x	
SI-3	**Malicious Code Protection**	x	x		x	x
SI-4	**System Monitoring**	x		x	x	x
SI-4(17)	*System Monitoring | Integrated Situational Awareness*				x	x
SI-4(19)	*System Monitoring | Risk for Individuals*				x	x
SI-5	**Security Alerts, Advisories, and Directives**	x		x	x	x
SI-7	**Software, Firmware, and Information Integrity**		x		x	x
SI-7(14)	*Software, Firmware, and Information Integrity | Binary or Machine Executable Code*				x	x
SI-7(15)	*Software, Firmware, and Information Integrity | Code Authentication*					x
SI-12	**Information Management and Retention**	x				x
SI-20	**Tainting**		x		x	x
SR-1	**Policy and Procedures**	x		x	x	x
SR-2	**Supply Chain Risk Management Plan**	x				x
SR-3	**Supply Chain Controls and Processes**	x		x	x	x
SR-3(1)	*Supply Chain Controls and Processes | Diverse Supply Base*				x	x
SR-3(3)	*Supply Chain Controls and Processes | Sub-tier Flow Down*		x		x	x
SR-4	**Provenance**				x	x
SR-5	**Acquisition Strategies, Tools, and Methods**	x		x	x	x
SR-6	**Supplier Assessments and Reviews**				x	x
SR-7	**Supply Chain Operations Security**				x	x
SR-8	**Notification Agreements**	x			x	x
SR-9	**Tamper Resistance and Detection**				x	x
SR-10	**Inspection of Systems or Components**	x	x		x	x
SR-11	**Component Authenticity**	x		x	x	x
SR-11(1)	*Component Authenticity | Anti-counterfeit Training*	x			x	x
SR-11(2)	*Component Authenticity | Configuration Control for Component Service and Repair*	x			x	x
SR-11(3)	*Component Authenticity | Anti-counterfeit Scanning*				x	x
SR-12	**Component Disposal**	x			x	x
SR-13	**Supplier Inventory**				x	x

5674
5675

APPENDIX B: RISK EXPOSURE FRAMEWORK

There are numerous opportunities for vulnerabilities that impact the enterprise environment or the system/element to be intentionally or unintentionally inserted, created, or exploited throughout the supply chain. Exploitation of these vulnerabilities is known as a supply chain threat event. **A Threat Scenario is a set of discrete threat events, associated with a specific potential or identified existing threat source or multiple threat sources, partially ordered in time.** Developing and analyzing threat scenarios can help organizations have a more comprehensive understanding of the various types of threat events that can occur and lay the ground work for analyzing the likelihood and impact a specific event or events would have on an organization. Conducting this analysis is a useful way to discover gaps in controls and to identify and prioritize appropriate mitigating strategies.[19]

Threat scenarios are generally used in two ways:

- To translate the often disconnected information garnered from a risk assessment, such as described in [NIST SP 800-30 Rev. 1] , into a more narrowly scoped and tangible, story-like situation for further evaluation. These stories can help organizations to discover dependencies and additional vulnerabilities requiring mitigation and used for training; and

- To determine the impact that the successful exercise of a specific vulnerability would have on the organization and identify the benefits of mitigating strategies.

Threat scenarios serve as a key component of the organization's cyber supply chain risk management process described in Appendix C of this publication. An organization forms a threat scenario to analyze a disparate set of threat and vulnerability conditions to assemble a cohesive story that can be analyzed as part of a risk assessment. With a threat scenario defined, the organization can complete a risk assessment to understand how likely the scenario is and what would happen (i.e., the impact) as a result. Ultimately the analyzed components of a threat scenario are used to reach a risk determination which represents the organization's conclusion on its level of exposure to a cyber supply chain risk.

Once a risk determination has been made – the organization will determine a path for responding to the risk using the Risk Exposure Framework. Within the Risk Exposure Framework – organizations will document the threat scenario, the risk analysis, as well as the identified a risk response strategy and any associated C-SCRM controls.

This appendix provides an example of a Risk Exposure Framework for C-SCRM that can be used by organizations to develop their own, tailored Risk Exposure Framework for potential and identified threats that best suits their needs. It contains five examples of how this framework may be used. The examples differ slightly in their implementation of the framework so as to show how the framework may be tailored by an organization. Each example identifies one or more vulnerabilities, describes a specific threat source, identifies the expected impact on the organization, and proposes SP 800-161, Rev. 1 C-SCRM controls that would help mitigate the resulting risk.

[19] Additional example threat scenarios and threat lists can be found in the ICT SCRM Task Force: Threat Scenarios Report, February 2021, https://www.cisa.gov/publication/ict-scrm-task-force-threat-scenarios-report. This report leveraged the 2015 version of the NIST SP 800-161.

RISK EXPOSURE FRAMEWORK

Step 1: Create a Plan for Developing and Analyzing Threat Scenarios

- Identify the purpose of the threat scenario analysis in terms of the objectives, milestones, and expected deliverables;
- Identify the scope of organizational applicability, level of detail, and other constraints;
- Identify resources to be used, including personnel, time, and equipment; and
- Define a Risk Exposure Framework to be used for analyzing scenarios.

Step 2: Characterize the Environment

- Identify core mission/business processes and key organizational dependencies;
- Describe threat sources that are relevant to the organization. Include the motivation and resources available to the threat source, if applicable;
- List known vulnerabilities or areas of concern (Note: Examples of areas of concern include the planned outsourcing of a manufacturing plant, the pending termination of a maintenance contract, or the discontinued manufacture of an element.);
- Identify existing and planned controls;
- Identify related regulations, standards, policies, and procedures; and
- Define an acceptable level of risk (risk threshold) per the organization's assessment of Tactics, Techniques, and Procedures (TTPs), system criticality, and a risk owner's set of mission or business priorities. The level of risk or risk threshold can be periodically revisited and adjusted to reflect the elasticity of the global supply chain, organizational changes, and new mission priorities.

Step 3: Develop and Select Threat Event(s) for Analysis

- List possible ways threat sources could exploit known vulnerabilities or impact areas of concern to create a list of events (Note: Historical data is useful in determine this information.);
- Briefly outline the series of consequences that could occur as a result of each threat event. These may be as broad or specific as necessary. If applicable, estimate the likelihood and impact of each event;
- Eliminate those events that are clearly outside the defined purpose and scope of the analysis;
- Describe in more detail the remaining potential threat events. Include the TTPs a threat source may use to carry out attacks (Note: The level of detail in the description is dependent on the needs of the organization.); and
- Select for analysis those events that best fit the defined purpose and scope of the analysis. More likely or impactful events, areas of concern to the organization, and an event that can represent several of the other listed events are generally useful candidates.

Step 4: Conduct an Analysis using the Risk Exposure Framework

- For each threat event, note any immediate consequences of the event and identify those organizational units and processes that would be affected, taking into account existing and planned controls and the extent to which those controls are able to effectively prevent, withstand, or otherwise mitigate the harm that could result from the threat event, and applicable regulations, standards, policies, and procedures;
- Estimate the impact these consequences would have on the mission/business processes, information, assets, as well as the organizational units or other stakeholders affected, preferably in quantitative terms from historical data and taking into account existing and planned controls, and applicable regulations, standards, policies, and procedures (Note: It may be beneficial to identify a "most likely" impact level and a "worst-case" or "100-year" impact level.); and

- Identify those organizational units, processes, information (access or flows), and/or assets that may or would be subsequently affected, the consequences and the impact levels, until each affected critical affected items has been analyzed, taking into account existing and planned controls, and applicable regulations, standards, policies, and procedures (e.g., If a critical server goes down, one of the first processes affected may be the technology support department, but if they determine a new part is needed to bring the server backup, the procurement department may become involved.).

Step 5: Determine C-SCRM Applicable Controls

- Determine if and which threat scenario events create a risk level that exceeds a risk owner's acceptable level of risk (risk threshold). (Note: In some cases, the level of acceptable risk may be dependent on the capability to implement, or the cost of, mitigating strategies.) Identify opportunities to strengthen existing controls or potential new mitigating controls. Using a list of standard or recommended controls can make this process simpler. This appendix uses the controls in Section 4 of NIST SP 800-161 Rev. 1.
- Estimate the effectiveness of existing and planned controls at reducing the risk of a scenario;
- Estimate the capability and resources needed (in terms of money, personnel, time) to implement potential new or strengthened controls; and
- Identify those C-SCRM controls or combinations of C-SCRM controls that could cause the estimated residual risk of a threat event to drop to an acceptable level in the most resource-effective manner, taking into account any rules or regulations that may apply (Note: Consideration should be given to the potential that one control will help mitigate the risk from more than one event, or that a control may increase the risk of a separate event.).

Step 6: Evaluate / Feedback

- Develop a plan to implement the selected controls and evaluate their effectiveness; and
- Evaluate the effectiveness of the Risk Exposure Framework and make improvements as needed.

5796
5797

Table B-1: Sample Risk Exposure Framework

Threat Scenario	**Threat**	
	Threat Event Description	*Describe possible ways threat sources could exploit known vulnerabilities or impact areas of concern to create a list of events.* Threat event: An event or situation that has the potential for causing undesirable consequences or impact.
	Threat Event Outcome	*Describe the outcome of the threat event.* Threat Event Outcome: The effect a threat acting upon a vulnerability has on the confidentiality, integrity, and/or availability of the organization's operations, assets, and/or individuals.
Organizational units / processes/information/ assets/stakeholders affected		*List the affected organizational units / processes/information/ assets/stakeholders affected.*
Risk	**Impact**	*Enter the estimate of the impact the outcome of the consequences would have on the mission/business processes, information, assets, as well as the organizational units or other stakeholders affected, preferably in quantitative terms from historical data and taking into account existing and planned controls, and applicable regulations, standards, policies, and procedures (Note: It may be beneficial to identify a "most likely" impact level and a "worst-case" or "100-year" impact level.)* The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system.
	Likelihood	*Enter the likelihood a specific event or events would have on an organization* Likelihood: Chance of something happening
	Risk Score (Impact x Likelihood)	*Enter the risk score by multiplying impact x likelihood.* *A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.*
	Acceptable Level of Risk	*Define an acceptable level of risk (risk threshold) per the organization's assessment of Tactics, Techniques, and Procedures (TTPs), system criticality, risk appetite and tolerance, and a risk owner's set strategic goals and objectives.* Acceptable Risk: A level of residual risk to the organization's operations, assets, or individuals that falls within the defined risk appetite and risk tolerance thresholds set by the organization.
Mitigation	**Potential Mitigating Strategies / C-SCRM Controls**	*List the potential mitigating risk strategies and any relevant C-SCRM controls.*

		C-SCRM Risk Mitigation: A systematic process for managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing risk response strategies to the cyber supply chain risks presented by the supplier, the supplied products and services, or the supply chain.
	Estimated Cost of Mitigating Strategies	*Enter estimated cost of risk mitigating strategies.*
	Change in Likelihood	*Identify potential changes in likelihood.*
	Change in Impact	*Identify potential changes in impact.*
	Selected Strategies	*List selected strategies to reduce impact.*
	Estimated Residual Risk	*Enter the estimated amount of residual risk* Residual Risk: Portion of risk remaining after security measures have been applied.

5798
5799

SAMPLE SCENARIOS

This appendix provides five example threat scenarios specific to the U.S. government using a fictitious 'ABC Company' and the Risk Exposure Framework described above. The examples purposely vary in level of specificity and detail to show that threat scenarios can be as broad or specific—as detailed or generic—as necessary. While these scenarios use percentages and basic scoring measures (High, Moderate, Low) for likelihood, impact, and risk, organizations may use any number of different units of measure (e.g., CVSS score, etc.). Additionally, these scenarios vary slightly in implementation of the risk response framework to show the Risk Exposure Framework can be adapted as needed.

SCENARIO 1: Influence or Control by Foreign Governments Over Suppliers[20]

Background

An organization has decided to perform a threat scenario analysis of its Printed Circuit Board (PCB) suppliers. The scenario will focus on the sensitivity of the business to unforeseen fluctuations in component costs.

Threat Source

ABC Company designs, assembles, and ships 3.5 million personal computers per year. It has a global footprint both in terms of customer and supply bases. Five years ago, in an effort to reduce the cost of goods sold, ABC Company shifted a majority of its PCB procurement to Southeast Asia. To avoid being single sourced, ABC Company finalized agreements with five different suppliers within the country and has enjoyed a positive partnership with each during this time.

Vulnerability

N/A

Threat Event Description

The organization has established the following fictitious threat for the analysis exercise: Last year, the country where ABC Company does most of their PCB business has seen a new regime take over the government. This regime has been more focused on improving finances and business environment within the country, allowing larger firms who set up headquarters and other major centers within country advantages to more easily and cost-efficiently do business with suppliers within the same region. In February of 2019, this now-corrupt regime has passed new legislation establishing an additional 20 percent tax on all electronic components and goods sold outside of the country. This new law was to take effect on June 1, 2019.

When the new law was announced, the current ABC Company inventory of PCBs was about 10 percent of yearly demand, which was the typical inventory level with which they were comfortable. Before June, ABC Company reached out to all five suppliers to order additional materials, but there was quickly a shortage due to higher demand from many foreign customers of these products. By June 1, the day the

[20] Scenario 1 prose is slightly modified (e.g., changed company names) from ICT SCRM Task Force: Threat Scenarios Report, February 2021, https://www.cisa.gov/publication/ict-scrm-task-force-threat-scenarios-report. This report leveraged the 2015 version of the NIST SP 800-161.

new tax law took effect, ABC Company had reached an inventory level of up to 15 percent of yearly demand.

Outcome

Between February and June, ABC Company also looked to partner with new suppliers, but there were several issues identified. One in every 10 new suppliers ABC Company reached out to required a lead time for ramping up to desired demand of anywhere from 6 months to 18 months. This would necessitate additional work on ABC Company's part, including testing samples of the supplier PCBs and finalizing logistical details, to monitoring supplier-side activities such as procurement of raw materials and acquisition of additional personnel, production space, etc. necessary to meet the new demand.

The second issue due to the current contracts with all five current suppliers in Southeast Asia involved meeting minimum demand requirements, in that ABC Company was committed to purchasing at minimum 100,000 PCB's per month for the duration of the contracts (which ranged anywhere from 3 months to 24 months in length). This would mean ABC Company could not easily avoid the cost implications of the new tax. Could ABC Company absorb the cost of the PCBs? With a 20 percent cost increase, this eroded the margins of a PC from 13.5 percent down to 4.5 percent on average. For some of the lower-margin ABC Company offerings, it would likely result in discontinuing the line and using the now more expensive PCB's on higher-end models that could carry more margin.

Organizational Units / Processes Affected

N/A

Potential Mitigating Strategies / C-SCRM Controls

Perform regular assessment and review of supplier risk[21]; Diversify suppliers not only by immediate location, but also by country, region and other factors; Build cost implications into supplier contracts, making it easier to part ways with suppliers when costs rise too high (whether by fault of the supplier or otherwise); Adjust desired inventory levels to better account for unexpected shortage of demand at critical times; and Employ more resources in countries or regions of key suppliers with the intent to source advanced notice of new legislature that may negatively affect business.

[21] Regular assessment and review of supplier risk mitigating strategy was added to original Scenario 1 text from ICT SCRM Task Force: Threat Scenarios Report, February 2021, https://www.cisa.gov/publication/ict-scrm-task-force-threat-scenarios-report. This report leveraged the 2015 version of the NIST SP 800-161.

5879

Table B-2: Scenario 1

Threat Scenario	**Threat Source**	Dynamic geopolitical conditions that impact the supply of production components for PCs	
	Vulnerability	Geographical concentration of suppliers for a key production component	
	Threat Event Description	ABC Company shifted a majority of its Printed Circuit Board (PCB) procurement to Southeast Asia to reduce cost of goods sold. In an effort to avoid being single sourced, ABC Company finalized agreements with five different suppliers within the country. The country in which ABC Company conducts most of their PCB business has seen a new regime assume governmental authority. In February of 2019, this now-corrupt regime passed legislation establishing an additional 20 percent tax on all electronic components and goods sold outside of the country. This law was to take effect on June 1, 2019. When the new law was announced, the current ABC Company inventory of PCBs was about 10 percent of yearly demand, at the typical level of inventory with which they were comfortable. Before June, ABC Company reached out to all five suppliers to order additional materials, but there was quickly a shortage due to higher demand from many foreign customers of these products. By June 1, the day the new tax law took effect, ABC Company had reached an inventory level up to 15 percent of annual demand.	
	Threat Event Outcome	ABC Company also looked to partner with new suppliers, but there were issues identified with this approach: 1) One out of every 10 new suppliers to which ABC Company reached out required a lead time to ramp up to desired demand of anywhere from 6 months to 18 months; and 2) Current contracts with all five active suppliers in Southeast Asia stipulated minimum demand requirements, meaning ABC Company was committed to purchasing a minimum of 100,000 PCB's per month for the duration of the contracts (which ranged anywhere from 3 months to 24 months in length). This would mean ABC Company could not easily avoid the cost implications of this new tax. With a 20 percent cost increase, the margins of a PC eroded from 13.5 percent to 4.5 percent, on average.	
Organizational units / processes affected		N/A	
Risk	**Impact**	High: $40,000,000 decline in PC product line profit	
	Likelihood	Moderate: 10% annualized probability of occurrence	
	Risk Score (Impact x Likelihood)	High: Inherent Risk Exposure equal to approx. $4,000,000 in product line profit	
	Acceptable Level of Risk	No greater than 10% probability of greater than $10,000,000 in product line profit	
Mitig	**Potential Mitigating Strategies / C-SCRM Controls**	Assess and review supplier risk to include FOCI [SR-6(1)], employ supplier diversity requirements [C-	Perform regular assessment and review of supplier risk; Diversify suppliers not just by immediate

		SCRM_PL-3(1)], employ supplier diversity [SCRM_PL-8(2)], and adjust inventory levels [CM-8]	location, but by country, region and other factors; Build cost implications into supplier contracts, making it easier to walk away from suppliers when costs rise too high (whether its fault of the supplier or not); Adjust desired inventory levels to better account for unexpected shortage of demand at critical times; and Employ more resources in countries or regions of key suppliers with the intent to source advanced notice of new legislature that may negatively affect business.
	Estimated Cost of Mitigating Strategies	N/A	
	Change in Likelihood	Low: 10% probability of occurrence	
	Change in Impact	Moderate: $2,000,000 in product line profit	
	Selected Strategies	Combination of strategies using the mitigation noted.	
	Estimated Residual Risk	Low: Residual risk exposure 0.02% of PC product line profit margin	

SCENARIO 2: Telecommunications Counterfeits

Background

A large organization, ABC Company, has developed a system that is maintained by contract with an external integration company. The system requires a common telecommunications element that is no longer available from the Original Equipment Manufacturer (OEM). The OEM has offered a newer product as a replacement which would require modifications to the system at a cost of approximately $1 million. If the element is not upgraded, the agency and system integrator would have to rely on secondary market suppliers for replacements. The newer product provides no significant improvement on the element currently being used.

ABC Company has decided to perform a threat scenario analysis to determine whether to modify the system to accept the new product or accept the risk of continuing to use a product that is no longer in production.

Environment

The environment is characterized as follows:

- The system is expected to last ten more years without any major upgrades/modifications and has a 99.9% uptime requirement.

- Over 1000 of the $200 elements are used throughout the system and approximately 10% are replaced every year due to regular wear-and-tear, malfunctions, or other reasons. The integrator has an approximate three-month supply on hand at any given time.
- The element is continuously monitored for functionality, and efficient procedures exist to reroute traffic and replace the element should it unexpectedly fail.
- Outages resulting from unexpected failure of the element are rare, localized, and last only a few minutes. More frequently, when an element fails, the system's functionality is severely reduced for approximately one to four hours while the problem is diagnosed and fixed or the element replaced.
- Products such as the element in question have been a common target for counterfeiting.
- The integrator has policies restricting the purchase of counterfeit goods and a procedure to follow if a counterfeit is discovered [Ref. SR-11].
- The integrator and acquiring agency have limited testing procedures to ensure functionality of the element before acceptance [Ref. SR-5(2)].

Threat Event

To support the threat scenario, the agency created a fictitious threat source described as a group motivated by profit with vast experience creating counterfeit solutions. The counterfeiter is able to make a high profit margin by creating and selling as genuine products that are visually identical to their genuine counterparts but which use lower-quality materials. They have the resources to copy most trademark and other identifying characteristics and insert counterfeits into a supply chain commonly used by the organization with little to no risk of detection. The counterfeit product is appealing to unaware purchasing authorities as it is generally offered at a discount, sold as excess inventory or as stockpile.

If an inferior quality element was inserted into the system, it would likely fail more often than expected, causing reduced functionality of the system. In the event of a large number of counterfeit products integrating with genuine parts into the system randomly, the number and severity of unexpected outages could grow significantly. The agency and integrator decided that the chances a counterfeit product could be purchased to maintain the system and the estimated potential impact of such an event were high enough to warrant further evaluation.

Threat Scenario Analysis

The person(s) purchasing the element from a supplier will be the first affected by a counterfeit product. Policy requires they attempt to purchase a genuine product from vetted suppliers. This individual would have to be led to believe that the product is genuine. As the counterfeit product in question is visually identical to the element desired, and at a discount, there is a high chance the counterfeit will be purchased. One will be tested to ensure functionality, and then the items will be placed into storage.

When one of the elements in the system needs replacing, an engineer will install a counterfeit, quickly test to ensure it is running properly, and record the change. It could take two years for the counterfeit product to fail, so up to 200 counterfeit elements could be inserted into the system before the first sign of failure. If all the regularly replaced elements are substituted for counterfeits and each counterfeit fails after two years, the cost of the system would increase by $160,000 in ten years. The requisite maintenance time would also cost the integration company in personnel and other expenses.

When a counterfeit fails, it will take approximately one to four hours to diagnose and replace the element. During this time, productivity is severely reduced. If more than one of the elements fails at the same time, the system could fail entirely. This could cause significant damage to agency operations and violate the

99.9% uptime requirements set forth in the contract. Plus, if it becomes determined that the element failed because it was counterfeit, additional costs associated with reporting the counterfeit would be incurred.

Mitigation Strategy

The following were identified as potential mitigating activities (from NIST SP 800-161 Rev. 1):

- Require developers to perform security testing/evaluation at all post-design phases of the SDLC [Ref. SA-11];
- Validate that the information system or system component received is genuine and has not been altered [Ref. SR-11];
- Incorporate security requirements into the design of information systems (security engineering) [Ref. PL-8, SC-36]; and
- Employ supplier diversity requirements [PL-8(2)].

Based on these controls, the agency was able to devise a strategy that would include:

- Acceptance testing: Examination of elements to ensure they are new, genuine, and that all associated licenses are valid. Testing methods include, where appropriate: physical inspection by trained personnel using digital imaging, digital signature verification, serial/part number verification, and sample electrical testing;
- Increasing security requirements into the design of the system by adding redundant elements along more critical paths (as determined by a criticality analysis) and in order to minimize the impact of an element failure; and
- Search for alternative vetted suppliers/trusted components.

It was determined that this strategy would cost less than accepting the risk of allowing counterfeits into the system or modifying the system to accept the upgraded element. The estimated cost for implementing a more rigorous acquisition and testing program was $80,000; the cost for increasing security engineering requirements was $100,000.

Table B-3: Scenario 2

Threat Scenario	**Threat Source**	Counterfeit telecommunications element introduced into supply chain
	Vulnerability	Element no longer produced by OEM Purchasing authorities unable / unwilling to identify and purchase only genuine elements
	Threat Event Description	Threat agent inserts their counterfeit element into a trusted distribution chain. → Purchasing authorities buy the counterfeit element. → Counterfeit elements installed into the system
	Threat Event Outcome	The element fails more frequently than before, increasing the number of outages
Organizational units / processes/information/ assets/stakeholders affected		Acquisitions Maintenance OEM / supplier relations Mission-essential functions
(Risk	**Impact**	Moderate: Element failure leads to 1-4-hour system downtime

	Likelihood	High: Significant motivation by threat actor and high vulnerability due to agency's inability to detect counterfeits with 25% annualized probability of premature component failure	
	Risk Score (Impact x Likelihood)	Medium: Significant short-term disruptions that lead downtime to exceed uptime threshold by 0.5% (e.g., 99.4% < 99.9% requirement)	
	Acceptable Level of Risk	Low: System must have less than 10% annualized probability of missing 99% uptime thresholds	
Mitigation	**Potential Mitigating Strategies / C-SCRM Controls**	Increase acceptance testing capabilities [C-SCRM_SA-9; C-SCRM_SA-10], increase security requirements in design of systems [C-SCRM_PL-2, and employ supplier diversity requirements [C-SCRM_PL-8(2)]	Modify the system to accept element upgrade
	Estimated Cost of Mitigating Strategies	$180,000	$1 million
	Change in Likelihood	Low: 8% annualized probability of component failure	
	Change in Impact	Low: Element failure causes failover to redundant system component – cost limited to maintenance and replacement	
	Selected Strategies	Agency-level examination and testing Place elements in escrow until they pass defined acceptance testing criteria Increase security engineering Search for multiple suppliers of the element	
	Estimated Residual Risk	Low: 8% annualized probability of component failures leading to system downtime (i.e., less than 99.9% uptime)	

SCENARIO 3: Industrial Espionage

Background

ABC Company, a semiconductor (SC) company used by the organization to produce military and aerospace systems, is considering a partnership with a KXY Co. to leverage their fabrication facility. This would represent a significant change in the supply chain related to a critical system element. A committee was formed including representatives from the organization, ABC Company, and the integration company to help identify the impact the partnership would have on the organization and risk-appropriate mitigating practices to enact when the partnership is completed.

Environment

The systems of concern are vital to the safety of military and aerospace missions. While not classified, the element that KXY would be expected to manufacture is unique, patented, and critical to the operational status of the systems. Loss of availability of the element while the system is operational could have significant, immediate impact across multiple agencies and the civilian populous, including loss of life

and millions of dollars in damages. An initial Risk Assessment was accomplished using [NIST SP 800-30 Rev. 1], and the existing level of risk for this is was given a score of "Moderate."

KXY currently produces a state-of-the-art, low-cost wafer fabrication with a primarily commercial focus. The nation-state in which KXY operates has a history of conducting industrial espionage to gain IP/technology. They have shown interest in semiconductor technology and provided a significant grant to KXY to expand into the military and aerospace markets. While KXY does not currently have the testing infrastructure to meet U.S. industry compliance requirements, the nation-state's resources are significant, including the ability to provide both concessions as well as incentives to help KXY meet those requirements.

The key area of concern was that the nation-state in which KXY operates would be able to use its influence to gain access to the element or the element's design.

The committee reviewed current mitigation strategies in place and determined that ABC Company, the integration company, and the organization had several existing practices to ensure that the system and all critical elements, as determined by a criticality analysis, met specific functionality requirements. For example, the system and critical elements are determined compliant with relevant industry standards. As part of their requirements under [NIST SP 800-53 Rev.5], the agency had some information protection requirements (Ref. PM-11). In addition, ABC Company had a sophisticated inventory tracking system that required that most elements to be uniquely tagged using RFID technology or otherwise identified for traceability (Ref. SR-4)).

Threat Scenario

Based on past experience, the organization decided that KXY's host nation would likely perform one of two actions if given access to the technology: sell it to interested parties, or insert/identify vulnerabilities for later exploitation. For either of these threat events to succeed, the host nation would have to understand the purpose of the element and be given significant access to the element or element's design. This could be done with cooperation of KXY's human resources department, through deception, or by physical or electronic theft. Physical theft would be difficult given existing physical control requirements and inventory control procedures. For a modified element to be purchased and integrated with the system, it would need to pass various testing procedures at both the integrator and agency levels. Testing methods currently utilized included radiographic examination, material analysis, electrical testing, and sample accelerated life testing. Modifications to identification labels/schemes would need to be undetectable in a basic examination. In addition, KXY would need to pass routine audits, which would check KXY's processes for ensuring the quality and functionality of the element.

The committee decided that, despite existing practices, there was a 30% chance that the host nation would have the motivation and ability to develop harmful modifications to the element without detection, exploit previously unknown vulnerabilities, or provide the means for one of their allies to do the same. This could result in a loss of availability or integrity of the system, causing significant harm. Using information from an initial Risk Assessment accomplished using [NIST SP 800-30 Rev. 1], the committee identified this as the worst-case scenario with an impact score of "High."

There is approximately a 40% chance that the host nation could and would sell the technology to interested parties, resulting in a loss of technological superiority. If this scenario occurred, friendly military and civilian lives could be at risk, intelligence operations would be damaged, and more money

would be required to invest in a new solution. The committee assigned an impact score for this scenario of "Moderate."

The committee determined that the overall combined risk score for the vulnerability of concern was "High."

Mitigating Strategies

Using NIST SP 800-161 Rev. 1 as a base, three broad strategies were identified by the committee: (1) improve traceability capabilities, (2) increase provenance and information requirements, and (3) choose another supplier. These three options were analyzed in more detail to determine specific implementation strategies, their impact on the scenarios, and their estimated cost to implement. (Specific technologies and techniques are not described in this case but would be useful in an actual threat scenario evaluation).

Improve traceability and monitoring capabilities

- CM-8 - SYSTEM COMPONENT INVENTORY
- IA-1 - POLICY AND PROCEDURES
- SA-10 - DEVELOPER CONFIGURATION MANAGEMENT
- SR-8 - NOTIFICATION AGREEMENTS
- SR-4 - PROVENANCE

Cost = 20 % increase
Impact = 10 % decrease

Increase provenance and information control requirements

- AC-21 - INFORMATION SHARING
- SR-4 - PROVENANCE

Cost = 20 % increase
Impact = 20 % decrease

Choose another supplier

- SR-6- SUPPLIER ASSESSMENTS AND REVIEWS

Cost = 40 % increase
Impact = 80 % decrease

Based on this analysis, the committee decided to implement a combination of practices:

- Develop and require unique, difficult-to-copy labels or alter labels to discourage cloning or modification of the component [Ref. SR-3(2)];
- Minimize the amount of information that is shared to suppliers. Require that the information be secured [Ref. AC-21]; and
- Require provenance be kept and updated throughout the SDLC [Ref. SR-4].

With this combination of controls, the estimated residual risk was determined to be equivalent with the existing risk without the partnership at a cost increase that is less than if the organization had changed suppliers.

6100 **Table B-4: Scenario 3**
6101

Threat Scenario	**Threat Source**	Nation-state with significant resources looking to steal IP		
	Vulnerability	Supplier considering partnership with company that has relationship with threat source		
	Threat Event Description	Nation-state helps KXY meet industry compliance requirements. ABC Company partners with KXY to develop chips		
	Existing Practices	Strong contractual requirements as to the functionality of the system and elements Comprehensive inventory tracking system at ABC Company Industry compliance requirements		
	Threat Event Outcome	Nation-state extracts technology threat actor, modifies technology, or exploits previously unknown vulnerability		
Organizational units / processes/information/ assets/stakeholders affected		KXY Supplier ABC Company integrator functionality testing Technology users Other federal agencies / customers		
Risk	**Impact**	Technology modified / vulnerabilities exploited – High	Technology sold to interested parties – Moderate	
	Likelihood	Moderate	Moderate	
	Risk Score (Impact x Likelihood)	High		
	Acceptable Level of Risk	Moderate		
Mitigation	**Potential Mitigating Strategies / C-SCRM Controls**	**(1) Improve traceability and monitoring capabilities**	**(2) Increase provenance and information control requirements**	**(3) Choose another supplier**
	Estimated Cost of Mitigating Strategies	20% increase	20% increase	40% increase
	Change in Likelihood	Moderate → Low		
	Change in Impact	High → Moderate		
	Selected Strategies	Develop and require unique, difficult-to-copy labels or alter labels to discourage cloning or modification of the component [C-SCRM_PE-3] Minimize the amount of information that is shared to suppliers. Require that the information be secured [C-SCRM AC-21] Require provenance be kept and updated throughout the SDLC [C-SCRM_SR-4]		
	Estimated Residual Risk	Moderate – The residual risk was determined to be equivalent with the existing risk without the partnership		

6102
6103

SCENARIO 4: Malicious Code Insertion

Background

ABC Company has decided to perform a threat scenario analysis on a traffic control system. The scenario is to focus on software vulnerabilities and should provide general recommendations regarding mitigating practices.

Environment

The system runs nearly automatically and uses computers running a commonly available operating system along with centralized servers. The software was created in-house and is regularly maintained and updated by an integration company on contract for the next five years. The integration company is large, frequently used by ABC Company in a variety of projects, and has significant resources to ensure that the system maintains its high availability and integrity requirements.

Threats to the system could include loss of power to the system, loss of functionality, or loss of integrity causing incorrect commands to be processed. Some threat sources could include nature, malicious outsiders, and malicious insiders. The system is equipped with certain safety controls such as backup generator power, redundancy of design, and contingency plans if the system fails.

Threat Event

ABC Company decided that the most concerning threat event would result from a malicious insider compromising the integrity of the system. Possible attacks could include the threat actor inserting a worm or a virus into the system, reducing its ability to function, or they could manually control the system from one of the central servers or by creating a back-door in the server to be accessed remotely. Depending on the skillfulness of the attack, an insider could gain control of the system, override certain fail-safes, and cause significant damage.

Based on this information, ABC Company developed the following fictitious threat event for analysis:

> *John Poindexter, a disgruntled employee of the integration company, decides to insert some open source malware into a component of the system. He then resigns from the firm, leaving no traceability of his work. The malware has the ability to call home to John and provide him access to stop or allow network traffic at any or all 50 of the transportation stations. As a result, unpredictable, difficult-to-diagnose disruptions would occur, causing significant monetary losses and safety concerns.*

After a Risk Assessment was accomplished using [NIST SP 800-30 Rev. 1], management decided that the acceptable level of risk for this scenario was "Moderate."

Threat Scenario Analysis

If John were successful, a potential course of events could occur as follows:

> John conducts a trial run, shutting off the services of one station for a short time. It would be discounted as a fluke and have minimal impact. Later, John would create increasingly frequent disruptions at various stations. These disruptions would cause anger among employees and

customers and some safety concerns. The integration company would be made aware of the problem and begin to investigate the cause. They would create a workaround, and make the assumption there was a bug in the system. However, because the malicious code would be buried and difficult to identify, the integration company wouldn't discover it. John would then create a major disruption across several transportation systems at once. The workaround created by the integration company would fail due to the size of the attack, and all transportation services would be halted. Travelers would be severely impacted, and the media alerted. The method of attack would be identified, and the system modified to prevent John from accessing the system again. However, the underlying malicious code would remain. Revenue would decrease significantly for several months. Legal questions would arise. Resources would be invested in assuring the public that the system was safe.

Mitigating Practices

ABC Company identified the following potential areas for improvement:

- Establish and retain identification of supply chain elements, processes, and actors [SR-4];
- Control access and configuration changes within the SDLC and require periodic code reviews [AC-1, AC-2, CM-3];
- Require static code testing [RA-9]; and
- Incident Handling [IR-4].

Table B-5: Scenario 4

Threat Scenario	**Threat Source**	Integrator– Malicious Code Insertion
	Vulnerability	Minimal oversight of integrator activities - no checks and balances for any individual inserting a small piece of code
	Threat Event Description	Disgruntled employee of an Integrator company inserts malicious functionality into traffic navigation software, and then leaves the ABC Company
	Existing Practices	Integrator: peer-review process Acquirer: Contract that sets down time, cost, and functionality requirements
	Threat Event Outcome	50 large metro locations and 500 instances affected by malware. When activated, the malware causes major disruptions to traffic
Organizational units / processes/information/ assets/stakeholders affected		Traffic Navigation System Implementation company Legal Public Affairs
Risk	**Impact**	High – Traffic disruptions are major and last for two weeks while a work-around is created. Malicious code is not discovered and remains a vulnerability
	Likelihood	High
	Risk Score (Impact x Likelihood)	High

	Acceptable Level of Risk	Moderate
Mitigation	**Potential Mitigating Strategies / C-SCRM Controls**	C-SCRM_AC-1; C-SCRM_AC-2; C-SCRM_CM-3; C-SCRM_IR-2; C-SCRM_SA-10; C-SCRM_SA-11
	Estimated Cost of Mitigating Strategies	$2.5 million
	Change in Likelihood	High → Low
	Change in Impact	High (no change)
	Selected Strategies	Combination of strategies using the mitigation noted
	Estimated Residual Risk	Moderate

SCENARIO 5: Unintentional Compromise

Background

Uninformed insiders replace components with more cost-efficient solutions without understanding the implications to performance, safety, and long-term costs.

ABC Company has concerns about its acquisition policies and has decided to conduct a threat scenario analysis to identify applicable mitigating practices. Any practices selected must be applicable to a variety of projects and have significant success within a year.

Environment

ABC Company acquires many different systems with varying degrees of requirements. Because of the complexity of the environment, ABC Company officials decide they should use a scenario based on an actual past event.

Threat Event

Using an actual event as a basis, the agency designs the following threat event narrative:

> Gill, a newly hired program manager, is tasked with reducing the cost of a $5 million system being purchased to support complex research applications in a unique physical environment. The system would be responsible for relaying information regarding temperature, humidity, and toxic chemical detection as well as storing and analyzing various data sets. There must not be any unscheduled outages more than 10 seconds long, or serious safety concerns and potential destruction of research will occur. ABC Company's threat assessment committee determined that the acceptable level of risk for this type of event has a score of 2/10.

Gill sees that a number of components in the system design are priced high compared with similar components he has purchased in the commercial acquisition space. Gill asks John, a junior engineer with the integration company, to replace several load balancer/routers in the system design to save costs.

Threat Scenario Analysis

ABC Company decides that there were three potential outcomes to the scenario:

1. It is determined that the modifications are inadequate before any are purchased (30 % chance, no impact);
2. It is determined that the modifications are inadequate during testing (40 % chance, low impact); or
3. The inadequacy of the modifications is undetected, the routers are installed in the system, begin to fail, and create denial of service incidents (30 % chance, high impact).

Mitigating Strategies

Three potential mitigating strategies were identified:

- Improve the existing training program [Ref. AT-1] and add configuration management controls to monitor all proposed changes to critical systems [Ref. CM-1];
- Improve the testing requirements [Ref. SA-11]; and
- Require redundancy and heterogeneity in the design of systems [Ref. SC-29, SC-36].

Adding configuration management controls would increase the likelihood that the modifications were rejected either at the initial stage or during testing, but it was determined that a $200,000 investment in training alone could not bring the level of risk to an acceptable level in the time required.

Improving the testing requirements would increase the likelihood of the modifications being rejected during testing, but it was determined that no amount of testing alone could bring the level of risk to an acceptable level.

Requiring redundancy and heterogeneity in the design of the system would significantly reduce the impact of this and other events of concern, but could double the cost of a project. In this scenario, it was determined that an investment of $2 million would be required to bring the risk to an acceptable level.

As a result of this analysis, ABC Company decides to implement a combination of practices:

- A mandatory, day-long training program for those handling the acquisition of critical systems and adding configuration management controls requiring changes be approved by a configuration management board (CMB) ($80,000 initial investment);
- $60,000 investment in testing equipment and software for critical systems and elements; and
- Redundancy and diversity of design requirements as deemed appropriate for each project.

It was determined that this combination of practices would be most cost-effective for a variety of projects and help mitigate the risk from a variety of threats.

6255 **Table B-6: Scenario 5**

Threat Scenario	**Threat Source**	Internal Employee – Unintentional Compromise		
	Vulnerability	Lax training practices		
	Threat Event Description	A new acquisition officer (AO) with experience in commercial acquisition is tasked with reducing hardware costs. The AO sees that a number of components are priced high and works with an engineer to change the purchase order		
	Existing Practices	Minimal training program that is not considered mandatory Basic testing requirements for system components		
	Threat Event Outcome	Change is found unsuitable before purchase	Change is found unsuitable in testing	Change passes testing, routers installed and start to fail, causing a denial of service situation
Organizational units / processes/information/ assets/stakeholders affected		None	Acquisitions	Acquisitions, System, Users
Risk	**Impact**	None	Low	High
	Likelihood	Moderate: 30%	High: 40 %	Moderate: 30 %
	Risk Score (Impact x Likelihood)	None	Moderate	Moderate
	Acceptable Level of Risk	Low	Moderate	High
Mitigation	**Potential Mitigating Strategies / SCRM Controls**	Improve training program and require changes be approved by CMB.	Improve acquisition testing	Improve design of system
	Estimated Cost of Mitigating Strategies	$200,000	---	$2 million
	Change in Impact	None – No Change	Low – No Change	High → Low
	Change in Likelihood	30% →10%	40% →20%	30% -- No Change
	New Risk Score	None	Low	Moderate
	Selected Strategies	Require mandatory training for those working on critical systems and require approval of changes to critical systems by a configuration management board (Cost = $100,000)		
	Residual Risk:	Low		

APPENDIX C: C-SCRM ACTIVITIES IN THE RISK MANAGEMENT PROCESS

Risk management is a comprehensive process that requires organizations to: (i) frame risk (i.e., establish the context for risk-based decisions); (ii) assess risk; (iii) respond to risk once determined; and (iv) monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations. Figure 2-3 depicts interrelationships among the risk management process steps, including the order in which each analysis may be executed, and the interactions required to ensure that the analysis is inclusive of the various inputs at the organization, mission, and operations levels.

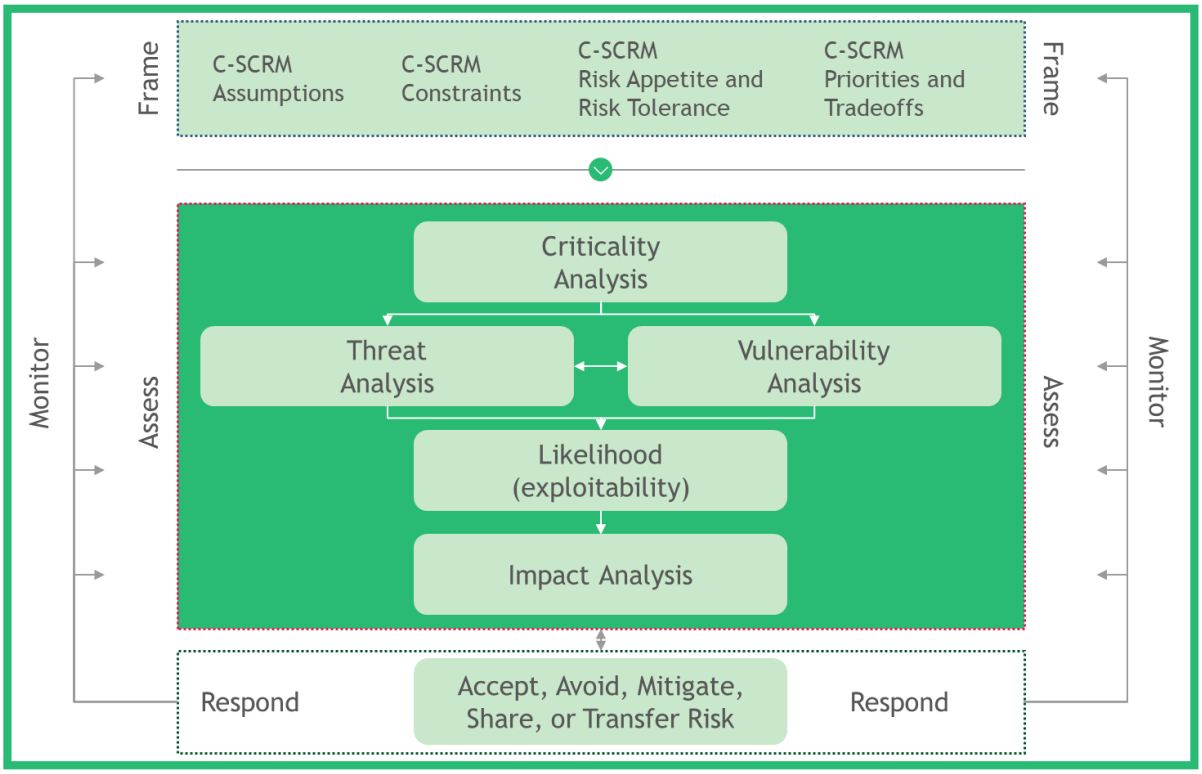
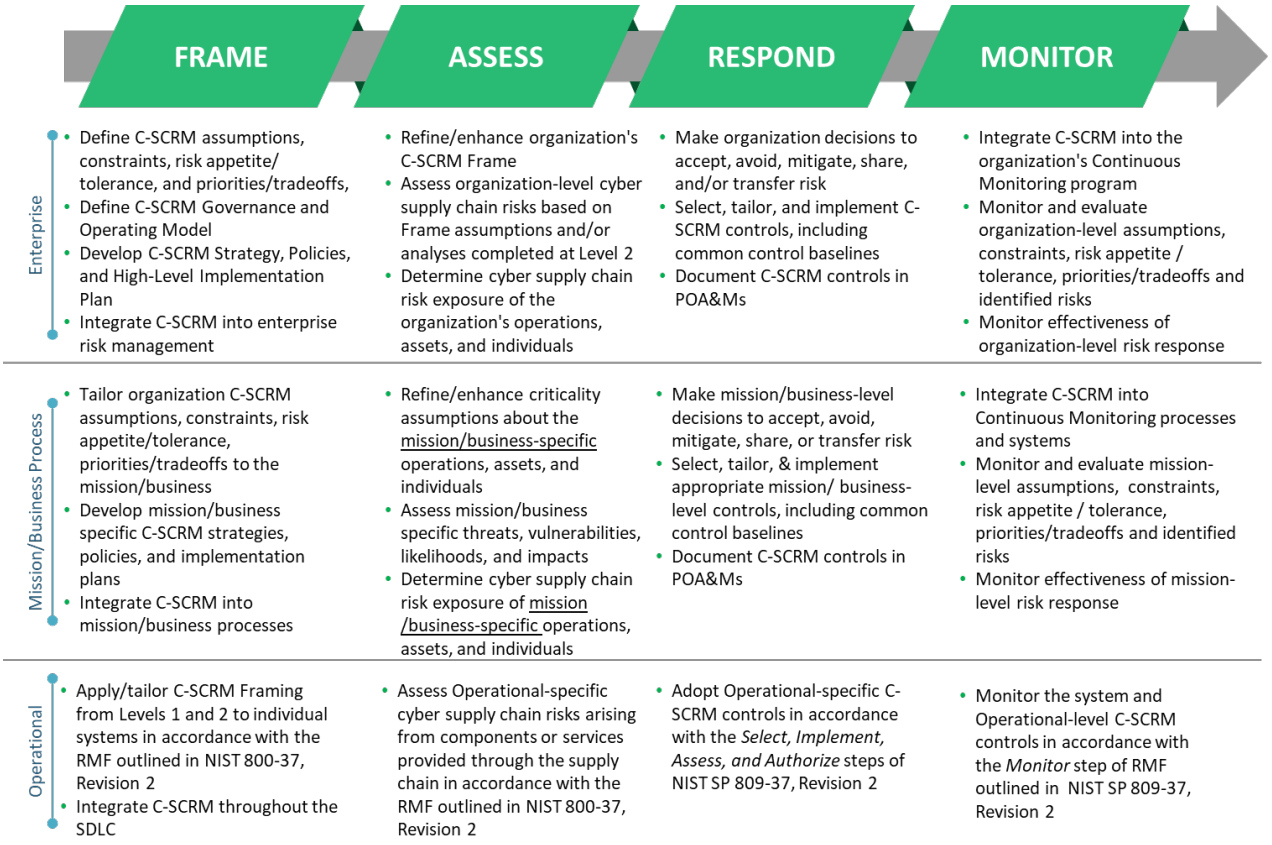


Fig. C-1: Cyber Supply Chain Risk Management (C-SCRM)

The steps in the risk management process (Frame, Assess, Respond, and Monitor) are iterative and not inherently sequential in nature. Different individuals may be required to perform the steps at the same time depending on a particular need or situation. Organizations have significant flexibility in how the risk management steps are performed (e.g., sequence, degree of rigor, formality, and thoroughness of application) and in how the results of each step are captured and shared—both internally and externally. The outputs from a particular risk management step will directly impact one or more of the other risk management steps in the risk management process.

Figure C-2 summarizes C-SCRM activities throughout the risk management process as they are performed within the three risk framework levels. The arrows between different steps of the risk management process depict simultaneous flow of information and guidance among the steps. Together the arrows indicate that the inputs, activities, and outputs are continuously interacting and influencing one another. More details are provided in the forthcoming subsections.

6280



6281

6282 **Fig. C-2: C-SCRM Activities in The Risk Management Process[22]**

6283

6284 Figure C-2 depicts interrelationships among the risk management process steps including the
6285 order in which each analysis is executed, and the interactions required to ensure the analysis is
6286 inclusive of the various inputs at the organization, mission, and operations levels.
6287
6288 The remainder of this section provides a detailed description of C-SCRM activities within the
6289 Frame, Assess, Respond, and Monitor steps of the Risk Management Process. The structure of
6290 subsections *Frame* through *Monitor* mirrors the structure of NIST SP 800-39, Sections 3.1-3.4.
6291 For each step of the Risk Management Process (i.e., Frame, Assess, Respond, Monitor), the
6292 structure includes Inputs and Preconditions, Activities, and Outputs and Post-Conditions.
6293 Activities are further organized into Tasks according to [NIST SP 800-39]. NIST SP 800-161
6294 cites the steps and tasks of the risk management process but rather than repeating any other
6295 content of [NIST SP 800-39], it provides C-SCRM-specific guidance for each step with its
6296 Inputs and Preconditions, Activities with corresponding Tasks, and Outputs and Post-Conditions.
6297 NIST SP 800-161 adds one task to the tasks provided in [NIST SP 800-39], under the Assess
6298 step: Task 2-0, *Criticality Analysis*.
6299

[22] More detailed information on the Risk Management Process can be found in Appendix C

Target Audience

The target audience for this appendix is those individuals with specific C-SCRM responsibilities for performing the supply chain risk management process across and at each level. Examples include those process/functional staff responsible for defining the frameworks and methodologies used by the rest of the organization (e.g., C-SCRM PMO Processes, Enterprise Risk Management, Mission/Business Process Risk Managers, etc.). Other personnel or entities are free to make use of the guidance as appropriate to their situation.

Organization-wide Risk Management & the RMF

Managing cyber supply chain risk requires a concerted and purposeful effort by organizations across organization, mission/business process, and operational-levels. This document describes two different but complementary risk management approaches which are iteratively combined to facilitate effective risk management across the 3 levels.

The first approach known as FARM consists of 4 steps: Frame, Assess, Respond, Monitor. FARM is primarily used at Levels 1 and 2 to establish the organization's risk context and inherent exposure to risk. Then, the risk context from Levels 1 and 2 iteratively informs activities performed as part of the second approach described in [NIST SP 800-37r2] The Risk Management Framework (RMF). The RMF predominantly operates at Level 3[23] – the operational level, and consists of 7 process steps: Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor[z]. Within the RMF, inputs from FARM at Levels 1 and 2 are synthesized as part of the RMF Prepare step, then iteratively applied, tailored and updated through each successive step of the RMF. Ultimately Level 1 and 2 assumptions are iteratively customized and tailored to fit the specific operational-level or procurement-action context. For example, an organization may decide on strategic priorities and threats at Level 1 (enterprise level), which inform the criticality determination of missions/business processes at Level 2, which in turn influence the system categorization, control selection, and control implementation as part of the RMF at Level 3 (operational-level). Information flow between the levels is bidirectional with aggregated Level 3 RMF outputs serving to update and refine assumptions made at Levels 1 and 2 on a periodic basis.

FRAME
Inputs and Preconditions

Frame is the step that establishes context for C-SCRM in all three levels. The scope and structure of the organizational cyber supply chain, the overall risk management strategy, specific program/project strategies and plans, and individual information systems are defined in this step. The data and information collected during Frame provides inputs for scoping and fine-tuning C-SCRM activities in other risk management process steps throughout the three levels. Frame is also where guidance in the form of frameworks and methodologies is established as part of the organization and mission/business process level risk management strategies. These frameworks

[23] The RMF does have some applications at Levels 1 and 2 such as the identification of common controls.

and methodologies provide bounds, standardization, and orientation for cyber supply chain risk management activities performed within later steps.

[NIST SP 800-39] defines risk framing as "the set of assumptions, constraints, risk tolerances, and priorities/trade-offs that shape an organization's approach for managing risk." Organization-wide and C-SCRM risk framing activities should iteratively inform one another. Assumptions the organization makes about risk should flow down and inform risk framing within C-SCRM activities (e.g., organization's strategic priorities). As the organization's assumptions about cyber supply chain risk evolve through the execution of C-SCRM activities, these assumptions should flow up and inform how risk is framed at the enterprise level (e.g., level of risk exposure to individual suppliers). Inputs into the C-SCRM risk framing process include, but are not limited to:

- Organization policies, strategies, and governance
- Applicable laws and regulations
- Agency critical suppliers and contractual services
- Organization processes (security, quality, etc.)
- Organization threats, vulnerabilities, risks, and risk tolerance
- Enterprise architecture
- Mission-level goals and objectives
- Criticality of missions/processes
- Mission-level security policies
- Functional requirements
- Criticality of supplied system/product components
- Security requirements

C-SCRM risk framing is an iterative process that also uses inputs from the other steps of the risk management processes (Assess, Respond, and Monitor) as inputs. Figure 2-5 depicts the Frame Step with its inputs and outputs along the three organizational levels. At the enterprise level, the organization will be concerned with conditions (i.e., assumptions, constraints, appetites and tolerances, and priorities and tradeoffs) that are broadly applicable across the organization and focus on contextualizing cyber supply chain risk to the organization's strategic goals and objectives. At the mission/business process level, frame activities focus on the individual mission and business process segments (e.g., assumptions about a technology assets or service provider's role in enabling enterprise-level objectives to be met). Level 2 frame activities take cyber supply chain risk conditions framed at Level 1, and tailor and contextualize them to reflect the role cyber supply chain risk has in each individual mission/business process to meet operational objectives. Finally, at Level 3, conditions outlined at Levels 1 and 2 iteratively inform each step of the RMF process. Beginning with the Prepare step, conditions outlined at Levels 1 and 2 are used to establish the context and priorities for managing cyber supply chain risk with respect to individual information systems, supplied system components, and system services providers. Then with each subsequent RMF step (Categorize through Monitor), these assumptions are iteratively updated and tailored to reflect applicable operational-level considerations. Information flow must be bi-directional between levels as insights discovered while performing lower level activities may update what is known about conditions outlined in higher levels.

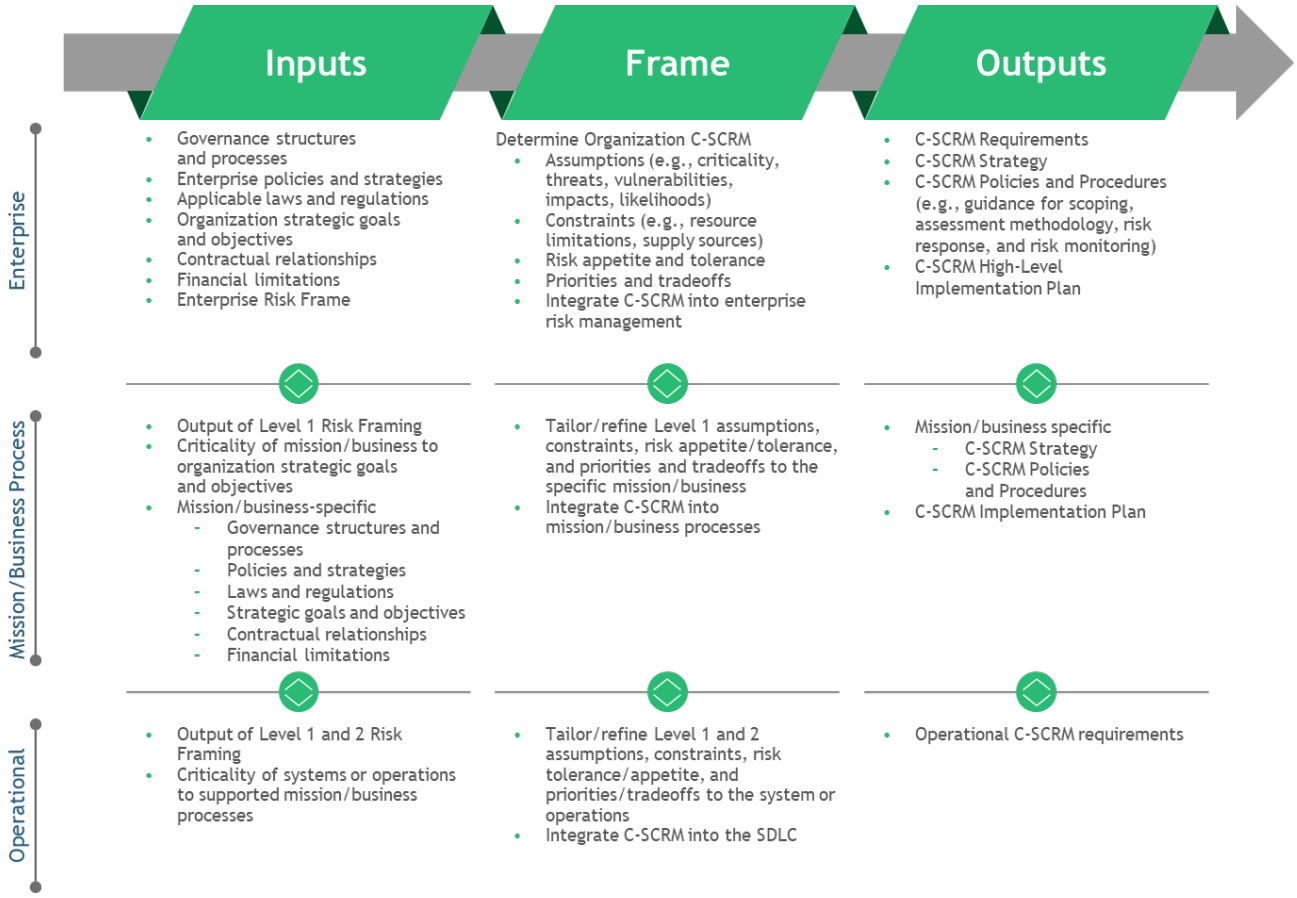


Fig. C-3: C-SCRM in the Frame Step[24]

Figures C-3 – C-6 depict inputs, activities, and outputs of the Frame Step distributed along the three risk management framework levels. The large arrows on the left and right sides of the activities depict the inputs and outputs to and from other steps of the Risk Management Process, with the arrow on the left depicting that steps are in constant interaction. Inputs into the Frame Step include inputs from other steps as well as inputs from the organization risk management process that are shaping the C-SCRM process. Up-down arrows between the levels depict flow of information and guidance from the upper levels to the lower levels and the flow of information and feedback from the lower levels to the upper levels. Together the arrows indicate that the inputs, activities, and outputs are continuously interacting and influencing one another.

As the Frame step is used to define the cyber supply chain risk conditions, organizations may find that Frame activities are performed relatively less often than the latter steps of the FARM process. Organizations may re-perform Frame activities at defined intervals (e.g., annually, bi-

[24] More detailed information on the Risk Management Process can be found in Appendix

annually) or based on defined triggers (e.g., based on business changes and/or new or updated insights from other levels).

Activities

RISK ASSUMPTIONS

TASK 1-1: Identify assumptions that affect how risk is assessed, responded to, and monitored within the organization.

Supplemental Guidance

As a part of identifying cyber supply chain risk assumptions within the broader Risk Management process (described in [NIST SP 800-39]), agencies should do the following:

- Develop an organization-wide C-SCRM policy;
- Identify which mission and business processes and related components are critical to the organization to determine the **criticality**;
- Define which mission and business processes and information systems compose the cyber supply chain, including relevant contracted services and commercial products;
- Prioritize the application of risk treatment for these critical elements, considering factors such as but not limited to national and homeland security concerns, FIPS 199 impact level, scope of use, or interconnections/interdependencies to other critical processes and assets;
- Identify, characterize, and provide representative examples of **threat sources**, **vulnerabilities**, **consequences/impacts**, and **likelihood** determinations related to cyber supply chain;
- Define C-SCRM mission, business, and operational-level requirements;
- Select appropriate cyber supply chain risk assessment methodologies, depending on organizational governance, culture, and diversity of the mission and business processes;
- Establish a method for the results of C-SCRM activities to be integrated into the overall agency Risk Management Process;
- Periodically review the cyber supply chain to ensure definition remains current as evolutions occur over time.

These supply chain risk assumptions should be aligned as applicable to the organization's broader set of risk assumptions defined as part of the enterprise risk management program. A key C-SCRM responsibility (e.g., of the C-SCRM PMO) is identifying which of those assumptions apply to the cyber supply chain risk context at each successive risk management framework level. If and when new C-SCRM assumptions are identified, these should be provided as updates to the enterprise risk assumptions as part of an iterative process.

Criticality

Critical processes are those processes, which if disrupted, corrupted or disabled, are likely to result in mission degradation or failure. Mission-critical processes are dependent on their supporting systems that in turn depend on critical components in those systems (hardware,

6451 software, and firmware). Mission-critical processes also depend on information and processes
6452 (performed by technology or people, to include in some instances, support service contractors),
6453 that are used to execute the critical processes. Those components and processes that underpin
6454 and enable mission-critical processes or deliver defensive—and often commonly shared—
6455 processes (e.g., access control, identity management, and crypto) and unmediated access (e.g.,
6456 power supply) should also be considered critical. A criticality analysis is the primary method by
6457 which mission-critical processes, associated systems/components, and enabling infrastructure
6458 and support services are identified and prioritized. The criticality analysis also involves
6459 analyzing critical suppliers which may not be captured by internal criticality analysis (e.g.,
6460 supply chain interdependencies including 4th and 5th party suppliers)
6461
6462 Organizations will make criticality determinations as part of enterprise risk management
6463 activities based on the process outlined in [NISTIR 8179].[25] Where possible, C-SCRM should
6464 inherit those assumptions and tailor/refine them to include the C-SCRM context. In C-SCRM,
6465 criticality tailoring includes initial criticality analysis of particular projects, products, and
6466 processes in the supply chain in relation to critical processes at each Level. For example, at Level
6467 1 the enterprise may determine the criticality of holistic supplier relationships to the
6468 organization's overall strategic objectives. Then at Level 2, the organization may assess the
6469 criticality of individual suppliers, products and services to specific mission/business processes
6470 and strategic/operational objectives. Finally, at Level 3, the organization may assess the
6471 criticality of the supplied product or service to specific operational state objectives of the
6472 information systems.
6473
6474 Organizations may begin by identifying key supplier-provided products or services which
6475 contribute to the operation and resiliency of organizational processes and systems. The criticality
6476 determination may be based on the role of each supplier, product, or service in achieving the
6477 required strategic or operational objective of the process or system. Requirements, architecture,
6478 and design inform the analysis and help identify the minimum set of supplier-provided products
6479 and/or services required for operations (i.e., at organization, mission/business process, and
6480 operational-levels). The analysis combines top-down and bottom-up analysis approaches. The
6481 top-down approach in this model enables the organization to identify critical processes and then
6482 progressively narrow the analysis to critical systems that support those processes, and finally to
6483 critical components which support the critical functions of those systems. The bottom-up
6484 approach progressively traces the impact of a malfunctioning, compromised, or unavailable
6485 critical component would have on the system, and in turn, on the related mission and business
6486 process.
6487
6488 Organizations performing this analysis should include agency system and cyber supply chain
6489 dependencies, to include critical 4th-party suppliers. For example, an organization may find
6490 cyber supply chain risk exposures that result from 3rd-party suppliers receiving critical input or
6491 services from a common 4th-party supplier.
6492
6493 Determining criticality is an iterative process performed at all levels during both Frame and
6494 Assess. In Frame, criticality determination is expected to be performed at a high level, using the

[25] NISTIR 8179: Criticality Analysis Process Model: Prioritizing Systems and Components

available information with further detail incorporated through additional iterations or at the Assess step. Determining criticality may include, but is not limited to, the following:

- Define criticality analysis procedures to ensure there is a set of documented procedures to guide the organization's criticality analysis across levels;
- Conduct organization and mission-level criticality analysis to identify and prioritize organization and mission objectives, goals and requirements;
- Conduct operational-level criticality analysis (i.e., systems and subsystems) to identify and prioritize critical workflow paths, system functionalities and capabilities;
- Conduct system and subsystem component-level criticality analysis to identify and prioritize key system and subsystem inputs (e.g., COTS products);
- Conduct detailed review (e.g., bottom-up analysis) of impacts and interactions between organization, mission, system/sub systems, and components/subcomponents to ensure cross-process interaction and collaboration.

Please note that criticality can be determined for existing systems or for future system investments, development, or integration efforts based on system architecture and design. It is an iterative activity that should be performed when a change warranting iteration is identified in the Monitor step.

Threat Sources

For C-SCRM, threat sources include: (i) adversarial threats such as cyber/physical attacks either to the supply chain or to an information system component(s) traversing the supply chain; (ii) accidental human errors; (iii) structural failures which include failure of equipment, environmental controls, resource depletion; and (iv) environmental threats such as geopolitical disruptions, pandemics, economic upheavals, and natural or man-made disasters. With regard to adversarial threats, [NIST SP 800-39] states that organizations provide a succinct characterization of the types of tactics, techniques, and procedures employed by adversaries that are to be addressed by safeguards and countermeasures (i.e., security controls) deployed at Level 1 (enterprise-level), at Level 2 (mission/business process level), and at Level 3 (information system/services level)—making explicit the types of threat sources to be addressed as well as making explicit the threat sources not being addressed by the safeguards/countermeasures.

Threat information can include but is not limited to historical threat data, factual threat data, or business entity (e.g., suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers) or technology-specific threat information. Threat information may come from multiple information sources, including the U.S. Intelligence Community (for federal agencies), DHS, CISA, the FBI, as well as open-source reporting such as news and trade publications, partners, suppliers, and customers. When applicable, organizations may rely on the Federal Acquisition Security Council's (FASC) Information Sharing Agency (ISA) for supply chain threat information in addition the aforementioned sources. As threat information may include classified intelligence, it is crucial that departments and agencies have the capabilities required to process classified intelligence. Threat information obtained as part of the Frame step should be used to document the organization's long-term assumptions about threat conditions based on its unique internal and external characteristics. During the Assess step,

updated information is infused into the risk assessment to account for short-term variations in threat conditions (e.g., due to geopolitical circumstances) as well as to obtain supply chain threat information that is specifically relevant and essential to inform the risk-based analysis and decision-making concerning the procurement of a given product or a service.

Information about cyber supply chain (such as supply chain maps) provides the context for identifying possible locations or access points for threat sources and agents to affect the cyber supply chain. The cyber supply chain threats are similar to the information security threats, such as disasters, attackers, or industrial spies. Table C-1 lists examples of cyber supply chain threat agents. Appendix D provides Risk Response Plans that provide examples of the Supply Chain Threat Sources and Threats listed in Table C-1.

Table C-1: Examples of Cyber Supply Chain Threat Sources/Agents

Threat Sources	Threat	Examples
Adversarial: Counterfeiters	Counterfeits inserted into cyber supply chain (see Appendix B Scenario 1)	Criminal groups seek to acquire and sell counterfeit cyber components for monetary gain. Specifically, organized crime groups seek disposed units, purchase overstock items, and acquire blueprints to obtain cyber components intended for sale through various gray market resellers to acquirers.[26]
Adversarial: Malicious Insiders	Intellectual property loss	Disgruntled insiders sell or transfer intellectual property to competitors or foreign intelligence agencies for a variety of reasons including monetary gain. Intellectual property includes software code, blueprints, or documentation.
Adversarial: Foreign Intelligence Services	Malicious code insertion (see Appendix B Scenario 3)	Foreign intelligence services seek to penetrate cyber supply chain and implant unwanted functionality (by inserting new or modifying existing functionality) into system to gather information or subverting[27] system or mission operations when system is operational.

[26] "Defense Industrial Base Assessment: Counterfeit Electronics," [*Defense Industrial Base Assessment: Counterfeit Electronics*].

[27] Examples of subverting operations include gaining unauthorized control to cyber supply chain or flooding it with unauthorized service requests to reduce or deny legitimate access to cyber supply chain.

[5]Information and Communications Technology Supply Chain Risk Management Task Force: Threat Evaluation Working. Group: Threat Scenarios Version 2.0

Adversarial: Terrorists	Unauthorized access	Terrorists seek to penetrate or disrupt the cyber supply chain and may implant unwanted functionality to obtain information or cause physical disablement and destruction of systems through the cyber supply chain.
Adversarial: Industrial Espionage/Cyber Criminals	Industrial Espionage/Intellectual Property Loss (see Appendix B Scenario 2)	Industrial spies/cyber criminals seek ways to penetrate cyber supply chain to gather information or subvert system or mission operations (e.g., exploitation of an HVAC contractor to steal credit card information).
Systemic: Legal/Regulatory	Legal/regulatory complications impact the availability of key supplier-provided products and/or services	Weak anti-corruption laws, lack of regulatory oversight, weak intellectual property considerations: this also includes the threats resulting from country-specific laws, policies, and practices intended to undermine competition and free market protections such as the requirement to transfer technology and intellectual property to domestic providers in a foreign country.[5]
Systemic Economic Risks	Business failure of a key supplier leads to supply chain disruption	Economic risks stem from threats to the financial viability of suppliers and the potential impact to the supply chain resulting from the failure of a key supplier as a result. Other threats to the supply chain that result in economic risks include, but are not limited to, vulnerabilities to cost volatility, reliance on single source suppliers, cost to swap out suspect vendors, and resource constraints due to company size.[5]
Environmental: Disasters	Geopolitical or natural disaster lead to supply chain disruption	Availability of key supply chain inputs is subject to disruptions from geopolitical upheavals or natural disasters. This is especially the case when suppliers share a common 4th-party supplier,

Structural: Hardware Failure	Inadequate capacity planning leads to outage in cloud platform	A vendor or supplier service without the appropriate capacity controls in place could be subject to disruptions in the event of unexpected surges in resource demand.
Accidental: Negligent Insiders	Configuration error leads to data exposure	Employees and contractors with access to information systems are prone to errors which could result in the disclosure of sensitive data. This is specifically true in cases where training lapses or process gaps increase the opportunities for errors.

Agencies can identify and refine C-SCRM-specific threats in all three levels. Table C-2 provides examples of threat considerations and different methods for use in characterizing cyber supply chain threats at different levels.

Table C-2: Supply Chain Threat Considerations

Level	Threat Consideration	Methods
Level 1	• Organization business and mission • Strategic supplier relationships • Geographical considerations related to the extent of the organization's cyber supply chain	• Establish common starting points for identifying cyber supply chain threat. • Establish procedures for countering organization-wide threats such as insertion of counterfeits into critical systems and components.
Level 2	• Mission and business processes • Geographic locations • Types of suppliers (COTS, external service providers, or custom, etc.) • Technologies used organization-wide	• Identify additional sources of threat information specific to organizational mission and business processes. • Identify potential threat sources based on the locations and suppliers identified through examining available agency cyber supply chain information (e.g., from supply chain map). • Scope identified threat sources to the specific mission and business processes, using the agency the cyber supply chain information. • Establish mission-specific preparatory procedures for countering threat adversaries/natural disasters.

Level 3	• SDLC	• Base the level of detail with which threats should be considered on the SDLC phase. • Identify and refine threat sources based on the potential for threat insertion within individual SDLC processes.

Vulnerabilities

A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source [FIPS 200], [NIST SP 800-34 Rev. 1], [NIST SP 800-53 Rev 4], [NIST SP 800-53A Rev. 4], [NIST SP 800-115]. Within the C-SCRM context, it is any weakness in the supply chain, provided services, system/component design, development, manufacturing, production, shipping and receiving, delivery, operation, and component end-of-life that can be exploited by a threat source. This definition applies to both the services/systems/components being developed and integrated (i.e., within the SDLC) and to the cyber supply chain, including any security mitigations and techniques, such as identity management or access control systems. Vulnerability assumptions made in the Frame step of the FARM process capture the organization's long-term assumptions about the organization's weaknesses that can be exploited or triggered by a threat source. These will become further refined and updated to reflect point-in-time variances during the Assess step. Organizations may make long-term cyber supply chain vulnerability assumptions about:

- The entities within supply chain itself (e.g., individual supplier relationships);
- The critical services provided through the supply chain which support the organization's critical missions and business processes;
- The products/systems/components provided through the supply chain and used within the SDLC (i.e., being developed and integrated);
- The development and operational environment directly impacting the SDLC; and
- The logistics/delivery environment that transports systems and components (logically or physically).

Vulnerabilities manifest differently across the 3 levels (i.e., organization, mission/business process, information system). At Level 1, vulnerabilities present as susceptibilities of the organization at-large due to managerial and operating structures (e.g., policies, governance, processes) as well as conditions in the supply chain (e.g., concentration of products or services from a single supplier) or critical enterprise processes (e.g., use of a common system across critical processes). At Level 2, vulnerabilities are specific to a mission/business process and result from its operating structures and conditions such as reliance on a specific system or supplier provided input, or service to achieve specific mission/business process operating objectives. Level 2 vulnerabilities may vary widely across the different mission/business processes. Within Level 3, vulnerabilities manifest as supplied product or operational-level weaknesses or deficiencies arising from the SDLC, system security procedures, internal controls,

6597 implementations, as well as system inputs or services provided through the supply chain (e.g.,
6598 system components, services).
6599
6600 Organizations should identify approaches to characterize cyber supply chain vulnerabilities
6601 consistent with the characterization of threat sources and events and with the overall approach
6602 employed by the organization for characterizing vulnerabilities. Vulnerabilities may be relevant
6603 to a single threat source or broadly applicable across threat sources (adversarial, structural,
6604 environmental, accidental). For example, a single point of failure in a network may be subject to
6605 disruptions caused by environmental threats (e.g., disasters) as well as adversarial threats
6606 (terrorists). Appendix B provides examples of cyber supply chain threats, based on [NIST SP
6607 800-30 Rev. 1, Appendix B].
6608
6609 All three levels should contribute to determining the organization's approach to characterizing
6610 vulnerabilities, with progressively more detail identified and documented in the lower levels.
6611 Table C-3 provides examples of considerations and different methods for use in characterizing
6612 cyber supply chain vulnerabilities at different levels.
6613

6614 **Table C-3: Cyber Supply Chain Vulnerability Considerations**

Level	Vulnerability Consideration	Methods
Level 1	• Enterprise mission/business • Holistic supplier relationships (e.g., system integrators, COTS, external services) • Geographical considerations related to the extent of the organization's cyber supply chain • Enterprise/Security Architecture • Criticality	• Examine agency cyber supply chain information including that from supply chain maps to identify especially vulnerable entities, locations, or organizations. • Analyze agency mission for susceptibility to potential supply chain vulnerabilities. • Examine 3rd party provider/ supplier relationships and interdependencies for susceptibility to potential supply chain vulnerabilities. • Review enterprise architecture and criticality to identify areas of weakness requiring more robust cyber supply chain considerations.
Level 2	• Mission and business processes • Geographic locations • Mission/process level supplier dependencies (e.g., outsourced or contracted services) • Technologies used	• Refine analysis from Level 1 based on specific mission and business processes and applicable threat and supply chain information. • If appropriate, use the National Vulnerability Database (NVD), including Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS), to characterize, categorize, and

		score vulnerabilities[28] or other acceptable methodologies. • Consider using scoring guidance to prioritize vulnerabilities for remediation.
Level 3	• Individual technologies, solutions, and services should be considered • Supply chain SDLC inputs such as system components or services	• Refine analysis based on inputs from related Level 2 missions and business processes. • Use CVEs where available to characterize and categorize vulnerabilities. • Identify weaknesses.

Consequences and Impact

Impact is the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system [NIST SP 800-53 Rev.5]. Impact estimated within the Frame step represents the organization's long-term assumptions about the effects different cyber events will have on its primary processes. These assumptions are updated and refined as part of the Assess step to ensure that point-in-time relevant information (e.g., market conditions)—which may alter the impact scope, duration, or magnitude—is appropriately reflected in the analysis.

When possible, organizations should inherit assumptions made by the organization on consequences and impact as part of enterprise risk management activities. For example, one of these activities is performing an impact analysis (BIA) on a periodic business to determine or revalidate mission-critical and mission-enabling processes, as part of the organization's continuity and emergency preparedness responsibilities. However, these assumptions may need to be developed if they do not yet exist. Organizations may maintain impact or loss libraries which capture the organization's standing assumptions about the impact of different cyber event types (e.g., disclosure, disruption, destruction, modification) on the organization's assets. These libraries may break down impact and loss into individual impact types (e.g., operational, reputational, regulatory/legal fines and penalties, IT recovery/replacement, direct financial, damage to critical infrastructure sector).

For C-SCRM, organizations should refine and update their consequences and impact assumptions to reflect the role that availability, confidentiality and integrity of supplier-provided products or services have on the organizational operations, assets, and individuals. For example, depending on its criticality, the loss of a key supplier-provided input or service may reduce the organization's operational capacity or completely inhibit its operations. In this publication,

[28] See https://nvd.nist.gov/

impact is always in relation to the organization's mission and includes the systems or components traversing the supply chain as well as the supply chain itself.

C-SCRM consequences and impact will manifest differently across all three levels in the risk management hierarchy. Impact determinations require a combined top-down and bottom-up approach. Table C-4 provides examples of how consequences and impact may be characterized at different levels of the organization:

Table C-4: Cyber Supply Chain Consequence & Impact Considerations

Level	Impact Considerations	Methods
Level 1	• General enterprise-level impact assumptions • Supplier criticality (e.g., holistic supplier relationships)	• Examine magnitude of exposure to individual entities within the supply chain. • Refine Level 2 analysis to determine aggregate Level 1 impact on the organization's primary function resulting from cyber events to and through the supply chain.
Level 2	• Process role in organization's primary function • Supplier criticality to mission/process (inputs and services)	For each type of cyber event: • Refine Level 3 analysis to determine aggregate mission/business process impact due to operational-level impacts from cyber events to and through the supply chain. • Examine supplier network to identify business/mission-level impacts due to events affecting individual supplier entities.
Level 3	• Criticality of upstream and downstream Level 2 processes • System criticality • Supplier criticality to system operations (system components and services)	• Examine the systems aggregated criticality to Level 1 and Level 2 primary processes • Examine the criticality of supplied system components or services to the system's overall function. • Examine supplier network to identify individual entities which may disrupt availability of critical system inputs or services.

Organizations should look to several sources for information that helps contextualize consequences and impact. Historical data is preferential and can be gathered by reviewing historical data for the agency, similar peer organizations, supplier organizations, or applicable industry surveys. Where gaps in historical data exist, organizations should consider the use of expert elicitation protocols (e.g., calibrated estimation training) which make use of the tacit knowledge of appropriate individuals across the organization. By interviewing well positioned experts (e.g., technology or mission/business owners of assets) organizations can tailor impact assumptions to reflect the organization's unique conditions and dependencies. NISTIR 8286

offers a more in-depth discussion of how different quantitative and qualitative methodologies can be used to analyze risk.

The following are examples of cyber supply chain consequences and impact:

- An earthquake in Malaysia reduces the amount of commodity Dynamic Random-Access Memory (DRAM) to 60 percent of the world's supply, creating a shortage for hardware maintenance and new design;
- Accidental procurement of a counterfeit part results in premature component failure, thereby impacting the organization's mission performance;
- Disruption in at a key cloud service provider resulting in operational downtime losses between $1.5M – $15M dollars.

Likelihood

In an information security risk analysis, likelihood is a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability [CNSSI 4009]. General likelihood assumptions should be inherited from the organization's enterprise risk management process then refined to account for C-SCRM specific implications however, the general assumptions may need developing if they do not yet exist. Likelihood analysis in the Frame step sets the organization's long-term assumptions about the relative likelihood of different adverse cyber events. Likelihood is subject to extreme short-term variations based on point-in-time conditions (i.e., internal and external) and thus must be updated and refined as part of the Assess step.

In adversarial cases a likelihood determination may be made using intelligence trend data, historical data, and expert intuition on (i) adversary intent; (ii) adversary capability; and (iii) adversary targeting. In non-adversarial cases (e.g., structural, environmental, accidental), likelihood determinations will draw on expert intuition and historical data. When available, historical data may help further reduce uncertainty about what cyber supply chain risks are probable to occur. Historical data may be sourced from internal sources (e.g., frequency of past security incidents, threat intelligence on threat activity levels) as well as external sources (e.g., peer org. data, info-sharing). Likelihood analysis can leverage many of the same expert elicitation protocols as consequences and impact. Similar to consequences and impact, likelihood determinations may rely on qualitative or quantitative form and draw on similar techniques. To ensure likelihood is appropriately contextualized for decision makers, organizations should make time-bound likelihood estimates for cyber events affecting the supply chain (e.g., likelihood within a given year).

Likelihood analysis will manifest differently across the three levels. Table C-5 captures some of the considerations and methods specific to each level:

6703 **Table C-5: Cyber Supply Chain Likelihood Considerations**

Level	Likelihood Consideration	Methods
Level 1	• General threat and likelihood assumptions for the organization • Level 2 and 3 likelihood findings • Overall engagement models with suppliers that alter opportunities for contact with threat sources	• Analyze critical national infrastructure implications which may increase the organization's target value. • Refine analyses from Levels 2 and 3 to determine aggregate exposure to threat source contact.
Level 2	• Mission/process level threat and likelihood assumptions • Mission/process level engagement model with suppliers (e.g., criticality of assets interacted with) • Level 3 findings for relevant systems	• Evaluate mission/business process level conditions which present opportunities for threat sources to come into contact with processes or assets via the supply chain. • Evaluate the aggregate supply chain threat conditions facing key systems relied upon by the mission/business process.
Level 3	• Organization system threat and likelihood assumptions • Supplier & system target value • Location & operating conditions • Supplier & system security policies, processes, and controls • Nature and degree of supplier contact with system (inputs, services)	• Analyze nature of system inputs coming through the supply chain into the SDLC which alter likelihood of encountering threat sources. • Evaluate the systems role in Level 1 and Level 2 processes which alter target value for potential adversaries. • Analyze supply chain characteristics (e.g., location of supplier) which may increase the likelihood that a system is affected by a threat source.

6704

6705 Agencies should determine which approach(es) they will use to determine the likelihood of a
6706 cyber supply chain compromise, consistent with the overall approach used by the agency's risk
6707 management process. Agencies should ensure that appropriate procedures are in place to
6708 thoroughly document any risk analysis assumptions leading to the tabulation of the final risk
6709 score, especially in cases where high or critical impact risks are involved. Visibility into
6710 assumptions may be critical in enabling decision makers to take action.
6711

RISK MANAGEMENT PROCESS CONSTRAINTS

TASK 1-2: Identify constraints[29] on the conduct of risk assessment, risk response, and risk monitoring activities within the organization.

Supplemental Guidance

Identify the following two types of constraints to ensure the cyber supply chain is integrated into the agency risk management process:

1. Agency constraints; and
2. Cyber supply chain-specific constraints.

Agency constraints serve as an overall input to framing the cyber supply chain policy at Level 1, mission requirements at Level 2, and system-specific requirements at Level 3. Table 2-5 lists the specific agency and cyber supply chain constraints. Cyber supply chain constraints, such as C-SCRM policy and C-SCRM requirements, may need to be developed if they do not exist.

Table C-6: Cyber Supply Chain Constraints

Level	Agency Constraints	Cyber Supply Chain Constraints
Level 1	• Enterprise policies, strategies, governance • Applicable laws and regulations • Mission and business processes • Organization processes (security, quality, etc.) • Resource limitations	• Organization C-SCRM policy based on the existing agency policies, strategies, and governance; applicable laws and regulations; mission and business processes; and organization processes. • Acquisition regulations and policy. • Available, mandated or restricted sources of supply or products.
Level 2	• Mission and business processes • Criticality of processes • Enterprise architecture • Mission-level security policies	• C-SCRM Mission/business requirements that are incorporated into mission/business processes and enterprise architecture. • Supplier service contracts, product warranties and liability agreements.

[29] Refer to [NIST SP 800-39], Section 3.1, Task 1-2 for a description of constraints in the risk management context.

Level 3	• Functional requirements • Security requirements	• Product and Operational-level C-SCRM capabilities. • Supplier-provided system component warranties and service agreements.

An organization's C-SCRM policy is a critical vehicle for directing C-SCRM activities. Driven by applicable laws and regulations, this policy should support applicable organization policies including acquisition and procurement, information security, quality, and supply chain and logistics. It should address goals and objectives articulated in the overall agency strategic plan, as well as specific mission and business processes and business goals, along with the internal and external customer requirements. It should also define the integration points for C-SCRM with the agency's Risk Management Process and SDLC.

C-SCRM policy should define C-SCRM-related roles and responsibilities of the agency C-SCRM team, any dependencies among those roles, and the interaction among the roles. C-SCRM-related roles will articulate responsibilities for collecting cyber supply chain threat intelligence, conducting risk assessments, identifying and implementing risk-based mitigations, and performing monitoring processes. Identifying and validating roles will help to specify the amount of effort required to implement the C-SCRM Plan. Examples of C-SCRM-related roles include:

- C-SCRM PMO that provides overarching cyber supply chain risk guidance to engineering decisions that specify and select cyber products as the system design is finalized;
- Procurement officer and maintenance engineering responsible for identifying and replacing the hardware when defective;
- Delivery organization and acceptance engineers who verify that the system component is acceptable to receive into the acquiring organization;
- System integrator responsible for system maintenance and upgrades, whose staff resides in the acquirer facility and uses system integrator development infrastructure and the acquirer operational infrastructure;
- System Security Engineer/Systems Engineer responsible for ensuring that information system security concerns are properly identified and addressed throughout the SDLC; and
- The end user of cyber systems/components/services.

C-SCRM requirements should be guided by C-SCRM policy(ies), as well as by the mission and business processes and their criticality at Level 2 and by known functional and security requirements at Level 3.

RISK APPETITE AND TOLERANCE

TASK 1-3: Identify the levels of risk appetite and tolerance for the organization.

Supplemental Guidance

Risk appetite represents the types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value [NISTIR 8286]. On the other hand, risk tolerance is the organization or stakeholder's readiness to bear the remaining risk after risk response in order to achieve its objectives, with the consideration that such tolerance can be influenced by legal or regulatory requirements [NISTIR 8286]. This definition is adapted from COSO, which states risk tolerance is the acceptable level of variation relative to achievement of a specific objective. Often, risk tolerance is best measured in the same units as those used to measure the related objective [COSO 2011]. Where applicable, organizations should align with risk appetite and tolerance assumptions and thresholds from the enterprise risk management process. For C-SCRM, these assumptions and thresholds should be contextualized to inform decisions in the C-SCRM domain. This may require C-SCRM define its own relevant C-SCRM-specific risk appetite and corresponding tolerance thresholds.

Risk appetite and tolerance strongly influence decisions made about C-SCRM across the three levels. Some organizations may define risk appetite and risk tolerance as part of their broader organization risk management activities (i.e., enterprise risk management). In organizations without a clearly defined risk appetite, Level 1 stakeholders should collaborate with organization leadership to define and articulate the organization's appetite for risk within the scope of the C-SCRM program's mandates. Organizations may choose to tailor risk appetite definitions to specific mission and business processes. In general, risk appetite at Level 1 may be set to empower the organization to meet its value objectives (e.g., high appetite for supplier risk in support of reducing operating costs by 5%). At Level 2 this may translate to relaxed C-SCRM governance structures and processes in alignment with this appetite threshold. Risk appetite definitions at lower levels should always be subject to the constraints provided at the higher levels.

With risk appetite defined, the organization should define its risk tolerance in order to operationalize the risk appetite across the organization. Risk tolerance should be defined for the organization as a whole as well as the specific mission and business processes. Organizations may use risk tolerance to inform cost/benefit decisions made about system components and services provided through the supply chain for systems throughout the SDLC. Risk Appetite and risk tolerance work together to guide C-SCRM decisions at various levels as the organization pursues its objectives.

Table C-7 shows additional examples of how risk appetite and risk tolerance statements work together to frame risk within an organization.

6808 **Table C-7: Risk Appetite & Risk Tolerance**

Level	Agency Constraints	Cyber Supply Chain Constraints
1	• **Low appetite** for risk with respect to market objectives	• **Low tolerance** (i.e., no more than 5% probability) for service provider downtime that causes system disruptions to exceed contractual service level agreements (SLAs) by more than 10%.
2	• **Low appetite** for appetite for risk with respect to production objectives	• **Moderate tolerance** (i.e., no more than 15% probability) for supply chain disruptions that cause production levels to fall below 80% of target threshold for non-military products. • **Near-zero tolerance (**i.e., no more than 5% probability) of supply chain disruptions that cause production levels to fall below 80% of target threshold for military products.
3.	• **Low appetite** for risk related to national security objectives	• **Low tolerance** (i.e., no more than 1% of contractor access authorizations) for inappropriate contractor access that exceeds authorized windows by more than 10% in systems with classified information.
4.	• **Low appetite** low appetite for risk related to operational objectives	• **Moderate tolerance** (i.e., no more than 15% probability) for system component failures causing non-critical system disruptions that exceed maximum allowable thresholds by more than 10%. • **Near-zero tolerance** (i.e., no more than 3% probability) for system component failures causing disruptions in critical systems that exceed maximum allowable thresholds by more than 10%.

6809

6810 To ensure leadership has the appropriate information when making risk-based decisions,
6811 organizations should establish metrics (e.g., Key Performance Indicators (KPIs), Key Risk
6812 Indicators (KRIs)) to measure performance against defined risk appetite and risk tolerance
6813 thresholds. Identification of corresponding data sources for measurement should play a key role
6814 in the organization's defined processes for setting and refining risk appetite and tolerance
6815 thresholds. Risk appetite and risk tolerance should be treated as dynamic thresholds by the

6816 organization. This requires periodic update and revision based on internal (e.g., strategy) and
6817 external (e.g., market, environmental) changes which impact the organization.
6818
6819 Organizations should consider cyber supply chain threats, vulnerabilities, constraints, and
6820 criticality when identifying the overall level of risk appetite and risk tolerance.[30]
6821
6822
6823 PRIORITIES AND TRADE-OFFS

6824 **TASK 1-4:** Identify priorities and trade-offs considered by the organization in managing risk.
6825
6826 **Supplemental Guidance**
6827
6828 Priorities and tradeoffs are closely linked to the organization's risk appetite and tolerance
6829 thresholds, which communicate the amount of risk that is acceptable and tolerable to the
6830 organization in pursuit of its objectives. Priorities will take the form of long-term strategic
6831 objectives or near-term strategic imperatives which alter risk decision calculus. From priorities
6832 and tradeoffs, C-SCRM then receives critical strategic context required for Response step
6833 activities such as Evaluation of Alternatives and Risk Response Decision. As a part of
6834 identifying priorities and trade-offs, organizations should consider risk appetite, risk tolerance,
6835 cyber supply chain threats, vulnerabilities, constraints, and criticality.
6836
6837 Priority and tradeoff considerations will manifest different across the 3 levels. Within Level 1,
6838 priority and tradeoff considerations may favor existing supplier relationships in established
6839 regions at the expense of new supplier cost advantages due to a desire to maintain confidence
6840 and stability. At Level 2, priority and tradeoff considerations may favor centralized C-SCRM
6841 governance models covering product teams in favor of greater security practice standardization.
6842 At Level 3, priorities and tradeoffs may favor system components/subcomponents produced in
6843 certain geographies in an effort to avoid environmental or geopolitical risks to the supply chain.
6844

6845 **Outputs and Post Conditions**

6846 Within the scope of NIST SP 800-39, the output of the risk framing step is the risk management
6847 strategy that identifies how organizations intend to assess, respond to, and monitor risk over
6848 time. This strategy should clearly include any identified C-SCRM considerations and should
6849 result in the establishment of C-SCRM-specific processes throughout the agency. These
6850 processes should be documented in one of three ways:
6851
6852 1. Integrated into existing agency documentation;
6853 2. A separate set of documents addressing C-SCRM; or
6854 3. A mix of separate and integrated documents based on agency needs and operations.
6855

[30] Federal Departments' and Agencies' governance structures vary widely (see [NIST SP 800-100, Section 2.2.2]). Regardless of the governance structure, individual agency risk decisions should apply to the agency and any subordinate organizations, but not in the reverse direction.

The following information should be provided as an output of the risk framing step, regardless of how the outputs are documented:

- C-SCRM Policy;
- Criticality including prioritized mission and business processes and FIPS 199 impact;
- Cyber supply chain risk assessment methodology and guidance;
- Cyber supply chain risk response guidance;
- Cyber supply chain risk monitoring guidance;
- C-SCRM mission/business requirements;
- Revised mission/business processes and enterprise architecture with C-SCRM considerations integrated;
- Operational-level C-SCRM requirements; and
- Acquisition security guidance/requirements.

Outputs from the risk framing step are enabling pre-requisites to effectively manage cyber supply chain risk and serve as inputs to the risk assessment, risk response, and risk monitoring steps.

ASSESS

Inputs and Preconditions

Assess is the step where assumptions, established methodologies and collected data is used to conduct a risk assessment. Numerous inputs (including criticality, risk appetite and tolerance, threats, and vulnerability analysis results; stakeholder knowledge; and policy, constraints, and requirements) are combined and analyzed to gauge the likelihood and impact of a cyber supply chain compromise. Assess step activities are used to update the organizations long-term risk-framing assumptions to account for near-term variations and changes.

A cyber supply chain risk assessment should be integrated into the overall organization risk assessment process. C-SCRM risk assessment results should be used and aggregated as appropriate to communicate potential or actual cyber supply chain risks relevant to each risk management framework level. Figure 2-6 depicts the Assess Step with its inputs and outputs along the three levels.

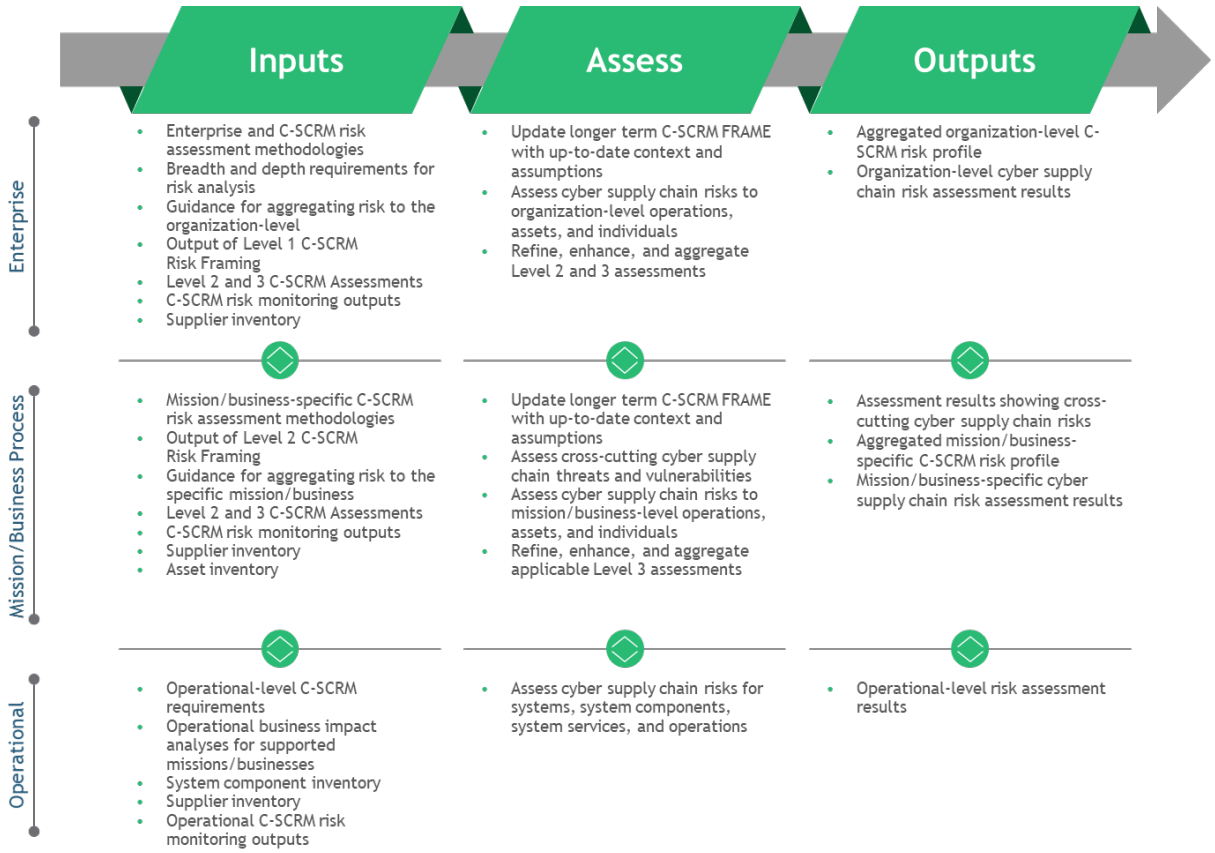


Fig. C-3: C-SCRM in the Assess Step[31]

Criticality, vulnerability, and threat analyses are essential to the supply chain risk assessment process. The order of activities begins with updating the criticality analysis to ensure the assessment is scoped to minimally include relevant critical mission and business processes and to understand the relevance and impact of cyber supply chain elements on these mission and business processes. As depicted in Figure C-4, vulnerability and threat analyses can then be performed, in any order, but should be performed iteratively to ensure that all applicable threats and vulnerabilities have been identified to understand which vulnerabilities may be more susceptible to exploitation by certain threats, and, if and as applicable, to associate identified vulnerabilities and threats to one or more mission and business processes or supply chain elements. Once viable threats and potential or actual vulnerabilities are assessed, this information will be used to evaluate the likelihood of exploitability—a key step to understanding impact. This is a synthesis point for criticality analysis, vulnerability analysis, and threat analysis and helps to further clarify and contextualize impact to support an informed and justifiable risk decision.

Activities

CRITICALITY ANALYSIS

[31] More detailed information on the Risk Management Process can be found in Appendix C

TASK 2-0: Update Criticality Analysis of mission and business processes, systems, and system components to narrow the scope (and resource needs) for C-SCRM activities to those most important to mission success.

Supplemental Guidance

Criticality analysis should include the cyber supply chain for both the organization and applicable suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, as well as relevant non-system services and products. Criticality analysis assesses the direct impact they each have on the mission priorities. The cyber supply chain includes the SDLC for applicable systems, services, and components because the SDLC defines whether security considerations are built into the systems/components or added after systems/components have been created.

Organizations should update and tailor criticality established during the Frame step of the risk management process, including FIPS 199 system. For low-impact systems, organizations should minimally assess criticality regarding interdependencies that systems may have with moderate or high-impact system(s). If systems are used extensively throughout the enterprise, organizations should determine the holistic impact of component failure or compromise in the low impact system.

In addition to updating and tailoring criticality, performing criticality analysis in the Assess Step may include the following:

- Refine the dependency analysis and assessment to update understanding of which components may require hardening given the system or network architecture;
- Obtain and review existing information that the agency has about critical systems/components such as locations where they are manufactured or developed, physical and logical delivery paths, information flows and financial transactions associated with these components, and any other available information that can provide insights into cyber supply chain of these components;[32]
- Update information about the cyber supply chain, historical data, and the SDLC to identify changes in critical cyber supply chain paths and conditions.

The outcome of the updated criticality analysis is a narrowed, prioritized list of the organization's critical processes, systems, and system components as well as a refined understanding of corresponding dependencies within the supply chain. Organizations can use the Criticality process in Section 2.2.1, Task 1-1, to update Criticality Analysis.

Because more information will be available in the Assess step, organizations can narrow the scope and increase the granularity of a criticality analysis. When identifying critical processes and associated systems/components and assigning them criticality levels, consider the following:

[32] This information may be available from a supply chain map for the agency or individual IT projects or systems. Supply chain maps are descriptions or depictions of supply chains including the physical and logical flow of goods, information, processes, and money upstream and downstream through a supply chain. They may include supply chain entities, locations, delivery paths, or transactions.

- Functional breakdown is an effective method of identifying processes, associated critical components, and supporting defensive functions;
- Dependency analysis is used to identify the processes on which critical processes depend (e.g., defensive functions such as digital signatures used in software patch acceptance) which become critical processes themselves;
- Identification of all access points to identify and limit unmediated access to critical function/components (e.g., least-privilege implementation);
- Value chain analysis to understand inputs, process actors, outputs and customers of services and products; and
- Malicious alteration or other types of supply chain compromise can happen throughout the SDLC.

The resulting list of critical processes and supply chain dependencies is used to guide and inform the vulnerability analysis and threat analysis in determining the initial C-SCRM risk as depicted in Figure 2-3. Cyber supply chain countermeasures and mitigations can then be selected and implemented to reduce risk to acceptable levels.

Criticality analysis is performed iteratively and may be performed at any point in the SDLC and concurrently by level. The first iteration is likely to identify critical processes and systems/components that have a direct impact on mission and business processes. Successive iterations will include information from the criticality analysis, threat analysis, vulnerability analysis, and mitigation strategies defined at each of the other levels. Each iteration will refine the criticality analysis outcomes and result in the addition of defensive functions. Several iterations are likely required to establish and maintain the criticality analysis results. Organizations should document or record the results of their criticality analysis and review and update this assessment on an annual basis at minimum.

THREAT AND VULNERABILITY IDENTIFICATION

TASK 2-1: Identify threats to and vulnerabilities in organizational information systems and the environments in which the systems operate.

Supplemental Guidance

In addition to threat and vulnerability identification, as described in [NIST SP 800-39] and [NIST SP 800-30 Rev. 1], organizations should conduct cyber supply chain threat analysis and vulnerability analysis.

Threat Analysis

For C-SCRM, a threat analysis provides specific and timely threat characterization of threat events (see Appendix C) and potential threat actors (e.g., Nation State) and threat vectors (e.g., 3rd party supplier), to inform management, acquisition, engineering, and operational activities

within an organization.[33] A variety of information can be used to assess potential threats, including open source, intelligence, and counterintelligence. Organizations should include, update and refine the threat sources and assumptions defined during the *Frame* step. The results of the threat analysis will ultimately support acquisition decisions, alternative build decisions, and development and selection of appropriate mitigations to be applied in the *Respond* step. The focus of Cyber supply chain threat analysis should be based on the results of the criticality analysis.

Agencies should use information available from existing incident management activities to determine whether they have experienced a cyber supply chain compromise and to further investigate such compromises. Agencies should define criteria for what constitutes a cyber supply chain compromise to ensure that such compromises can be identified as a part of post-incident activities, including forensics investigations. Additionally - at agency defined intervals – agencies should review other sources of incident information within the organization to determine whether in fact a supply chain compromise has occurred.

An cyber supply chain threat analysis should capture at least the following data:

- Observation of cyber supply chain-related attacks while they are occurring;
- Incident data collected post-cyber supply chain-related compromise;
- Observation of tactics, techniques, and procedures used in specific attacks, whether observed or collected using audit mechanisms; and
- Natural and man-made disasters before, during, and after occurrence.

Vulnerability Analysis

For C-SCRM, a vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source [FIPS 200], [NIST SP 800-34 Rev. 1], [NIST SP 800-53 Rev 4], [NIST SP 800-53A Rev. 4], [NIST SP 800-115].

A vulnerability analysis is an iterative process that informs risk assessment and countermeasure selection. The vulnerability analysis works alongside the threat analysis to help inform the impact analysis and to help scope and prioritize vulnerabilities to be mitigated.

Vulnerability analysis in the Assess Step should use the approaches defined during the Frame Step to update and refine assumptions about cyber supply chain vulnerabilities. Vulnerability analysis should begin by identifying vulnerabilities that are applicable to critical mission and business processes and systems/system components identified by the criticality analysis. An investigation of vulnerabilities may indicate the need to raise or at least reconsider the criticality levels of processes and components identified in earlier criticality analyses. Later iterations of

[33] Please note that threat characterization of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers may be benign.

the vulnerability analysis may also identify additional threats, or opportunities for threats, not considered in earlier threat assessments.

Table C-8 provides examples of applicable cyber supply chain vulnerabilities that can be observed within the three levels.

Table C-8: Examples of Cyber Supply Chain Vulnerabilities Mapped to the Organizational Levels

Level	Agency Constraints	Cyber Supply Chain Constraints
Level 1 – Organization	1) Deficiencies or weaknesses in organizational governance structures or processes such as a lack of C-SCRM Plan 2) Weaknesses in the supply chain itself (e.g., vulnerable entities, over-reliance on certain entities)	1) Provide guidance on how to consider dependencies on external organizations as vulnerabilities. 2) Seek out alternate sources of new technology including building in-house. leveraging trustworthy shared services/common solutions.
Level 2 – Mission/ Business	1) No operational process is in place for detecting counterfeits 2) No budget was allocated for the implementation of a technical screening for acceptance testing of supplied system components entering the SDLC as replacement parts 3) Susceptibility to adverse issues from innovative technology supply sources (e.g., technology owned or managed by third parties is buggy)	1) Develop a program for detecting tainted or counterfeit products and allocate appropriate budgets for putting in resources and training. 2) Allocate budget for acceptance testing – technical screening of components entering SDLC.
Level 3 – Operation	1) Discrepancy in system functions not meeting requirements, resulting in substantial impact to performance	1) Initiate engineering change. Malicious alteration can happen throughout the system life cycle to an agency system to address functional discrepancy and test correction for performance impact.

RISK DETERMINATION

TASK 2-2: Determine the risk to organizational operations and assets, individuals, other organizations, and the Nation if identified threats exploit identified vulnerabilities.

Supplemental Guidance

Organizations determine cyber supply chain risk by considering the likelihood that known threats exploit known vulnerabilities to and through the cyber supply chain and the resulting consequences or adverse impacts (i.e., magnitude of harm) if such exploitations occur. Organizations use threat and vulnerability information together with likelihood and consequences/impact information to determine C-SCRM risk either qualitatively or quantitatively. Outputs from the Risk Determination at Levels 1 and 2 should correspond directly with the RMF Prepare – Organization Level tasks described within [NIST 800-37r2], while risk assessments completed for Level 3 should correspond to directly with the RMF Prepare – Operational-level tasks.

Likelihood

Likelihood is a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability [CNSSI 4009]. Determining this likelihood requires the consideration of the characteristics of the threat sources, the identified vulnerabilities, and the organization's susceptibility to the cyber supply chain compromise, prior to and while the safeguards/mitigations are implemented. Likelihood determination should draw on methodologies defined as part of the Frame step, and update, refine, and expand any assumptions made about likelihood. For adversarial threats, this analysis should consider the degree of an adversary's capability and intent to interfere with the organization's mission. Cyber supply chain risk assessment should consider two views:

- The likelihood that one or more elements within the cyber supply chain itself is compromised. This may impact, for example, the availability of quality components or increase the risk of intellectual property theft; and
- The likelihood of the system or component within the supply chain being compromised, for example, by malicious code inserted into a system or an electric storm damaging a component.

In some cases, these two views may overlap or be indistinguishable, but both may have an impact on the agency's ability to perform its mission.

Likelihood determination should consider:

- Threat assumptions that articulate the types of threats the system or the component may be subject to, such as cybersecurity threats, natural disasters, or physical security threats
- Actual supply chain threat information such as adversaries' capabilities, tools, intentions, and targets

- Historical data about the frequency of supply chain events in peer or like organizations
- Internal expert perspectives on the probability systems or process compromise through the supply chain
- Exposure of components to external access (i.e., outside of the system boundary)
- Identified system, process, or component vulnerabilities
- Empirical data on weaknesses and vulnerabilities available from any completed analysis (e.g., system analysis, process analysis) to determine probabilities of cyber supply chain threat occurrence

Factors for consideration include the ease or difficulty of successfully attacking through a vulnerability and the ability to detect the method employed to introduce or trigger a vulnerability. The objective is to assess the net effect of the vulnerability, which will be combined with threat information to determine the likelihood of successful attacks within a defined time frame as part of the risk assessment process. The likelihood can be based on threat assumptions or actual threat data, such as previous breaches of the supply chain, specific adversary capability, historical breach trends, or frequency of breaches. The organization may use empirical data and statistical analysis to determine specific probabilities of breach occurrence, depending on the type of data available and accessible within the organization.

Impact

Organizations should begin impact analysis using methodologies and potential impact assumptions defined during the Frame step, determining the impact of a compromise and the impact of mitigating said compromise. Organizations need to identify the various adverse impacts of compromise, including: (i) the characteristics of the threat sources that could initiate the events; (ii) identified vulnerabilities; and (iii) the organizational susceptibility to such events based on planned or implemented countermeasures. Impact analysis is an iterative process performed initially when a compromise occurs, when mitigation approach is decided to evaluate the impact of change, and finally, in the ever-changing SDLC, when the situation/context of the system or environment changes.

Organizations should use the result of impact analysis to define an acceptable level of cyber supply chain risk for a given system. Impact is derived from criticality, threat, and vulnerability analysis results, and should be based on the magnitude of effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system [NIST SP 800-53 Rev. 5]. Impact is likely to be a qualitative measure requiring analytic judgment. Executive/decision-makers use impact as an input into the risk-based decisions whether to accept, avoid, mitigate, or share the resulting risks and the consequences of such decisions.

Organizations should document the overall results of cyber supply chain risk assessments in risk assessment reports.[34] Cyber supply chain risk assessment reports should cover risks in all three

[34] See [NIST SP 800-30 Rev. 1 Appendix K] for a description of risk assessment reports.

organizational levels as applicable. Based on the organizational structure and size, multiple cyber supply chain risk assessment reports may be required. Agencies are encouraged to develop individual reports at Level 1. For Level 2, agencies should integrate cyber supply chain risks into the respective mission-level Business Impact Assessments (BIA) and may want to develop separate mission-level cyber supply chain risk assessment reports. For Level 3, agencies may want to integrate cyber supply chain risks into the respective Risk Response Framework. Risk Response Frameworks at all three levels should be interconnected, reference each other when appropriate, integrate with the C-SCRM Plans, and comprise part of authorization packages.

Aggregation

Organizations may use risk aggregation to roll up several discrete or lower-level risks into a more general or higher-level risk [NIST SP 800-30 Rev. 1]. This is especially important for C-SCRM as organizations strive to understand their exposure to the cyber supply chain at operational-levels as well as at the relationship level (i.e., Level 1). Ultimately, organizations may wish to aggregate and normalize their C-SCRM risk assessment results with other enterprise risk assessments to develop an understanding of total risk exposure across risk types (e.g., financial, operational, legal/regulatory). To ease this process, organizations should maximize inheritance of common frameworks and lexicons from higher-order risk processes (e.g., enterprise risk management).

When dealing with discrete risks (i.e., non-overlapping), organizations can more easily develop a holistic understanding of aggregate Level 1 and 2 risk exposures. In many cases, however, organizations will find that risk assessments completed at lower levels contain overlapping estimates for likelihood and/or impact magnitude. In these cases, the sum of the pieces (i.e., risk exposure ratings at lower levels) is greater than the whole (i.e., aggregate risk exposure of the organization). To overcome these challenges, organizations can employ a variety of techniques. Organizations may elect to use visualizations or heat maps to demonstrate the likelihood and impact of risks relative to one another. When presenting aggregate risk as a number, organizations should ensure that assessments of risk produce discrete outputs by adopting mutually exclusive and collectively exhaustive (MECE) frameworks. MECE frameworks guide analysis of inputs (e.g., threats, vulnerabilities, impacts) and allow the organization to minimize overlapping assumptions and estimates. Instead of summing together risks from lower levels, organizations may elect to perform a new holistic assessment at an upper level leveraging the combined assessment results from lower levels. Doing so can help organizations avoid double counting of risk resulting in overestimation of their aggregate risk exposure. Organizations should apply discretion in aggregating risks so as to avoid risk aggregations that are difficult to explain (e.g., combining highly differentiated scenarios into a single number).

Quantitative methods offer distinct advantages for risk aggregation. Through the use of probabilistic techniques (e.g., Monte Carlo methods, Bayesian analysis), organizations can combine similar risks into a single, easily understood figure (e.g., dollars) in a mathematically defensible manner. Mutually exclusive and collectively exhaustive frameworks remain an important requirement for quantitative methods.

Outputs and Post Conditions

This step results in:

- Confirmed mission and business process criticality;
- Establishment of relationships between the critical aspects of the system's cyber supply chain infrastructure (e.g., SDLC) and applicable threats and vulnerabilities;
- Understanding of the likelihood and the impact of a potential cyber supply chain compromise;
- Understanding mission and system-specific risks;
- Documented cyber supply chain risk assessments for mission processes and individual systems; and
- Integration of relevant cyber supply chain risk assessment results into the organization risk management process.

RESPOND

Inputs and Preconditions

Respond is the step in which the individuals conducting risk assessment will communicate the assessment results, proposed mitigation/controls options, and the corresponding acceptable level of risk for each proposed option to the decision makers. This information should be presented in a manner appropriate to inform and guide risk-based decisions. This will allow decision makers to finalize appropriate risk response based on the set of options and taking into account the corresponding risk factors of choosing the various options. Sometimes an appropriate response is to do nothing and to monitor the adversary's activities and behavior to better understand the tactics and to attribute the activities.

Cyber supply chain risk response should be integrated into the overall organization risk response. Figure C-5 depicts the Respond Step with its inputs and outputs along the three organizational levels.

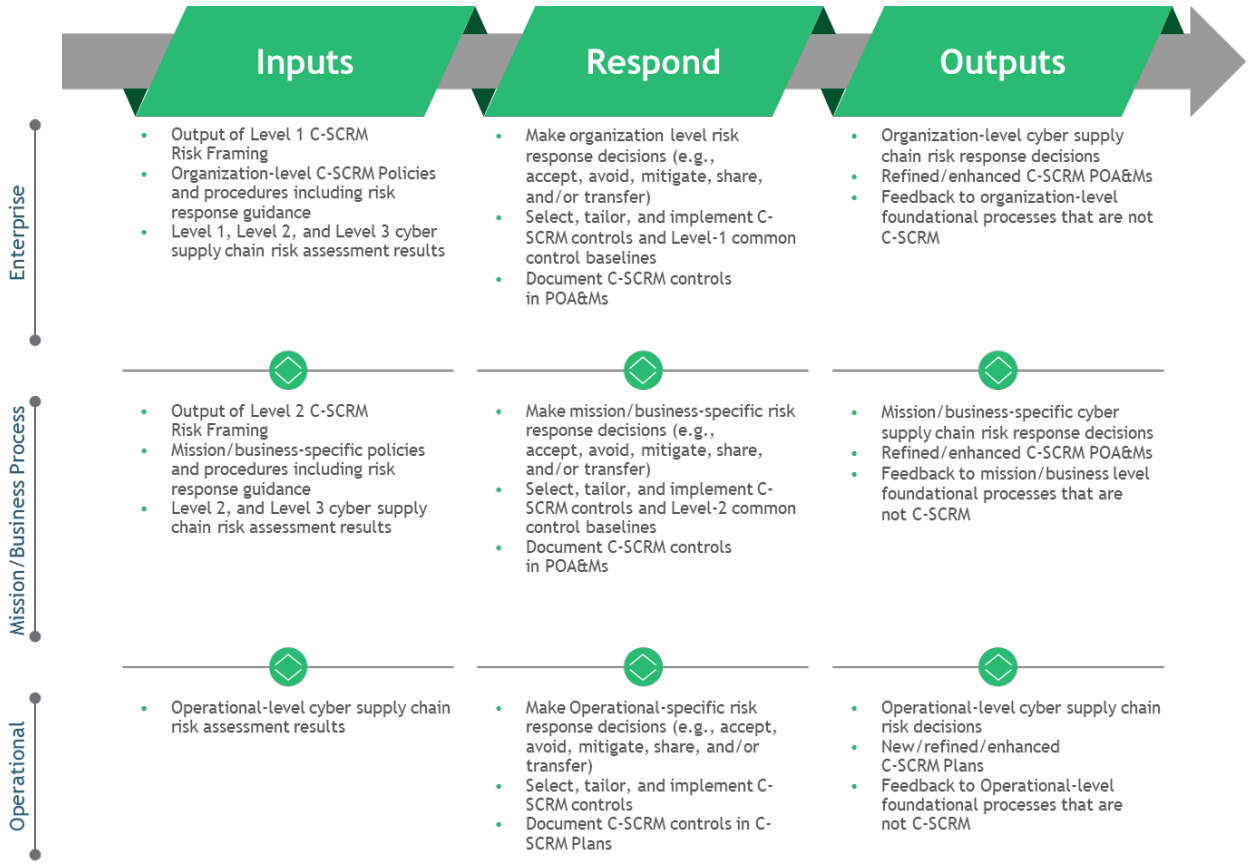


Fig. C-4: C-SCRM in the Respond Step[35]

Activities

RISK RESPONSE IDENTIFICATION

TASK 3-1: Identify alternative courses of action to respond to risk determined during the risk assessment.

Organization's risk response strategies will be informed by risk management strategies developed for the enterprise (i.e., Level 1) and mission/business process (i.e., Level 2). Risk response strategies will include general courses of action the organization may take as part of its risk response efforts (e.g., accept, avoid, mitigate, transfer or share). As part of mitigation efforts, organizations should select C-SCRM controls and tailor these controls based on the risk determination. C-SCRM controls should be selected for all three levels, as appropriate per findings of the risk assessments for each of the levels.

Many of the C-SCRM controls included in this document may be part of an IT security plan and should be incorporated as requirements in agreements made with third party providers. These controls are included because they apply to C-SCRM.

[35] More detailed information on the Risk Management Process can be found in Appendix C

This process should begin by determining acceptable risk to support the evaluation of alternatives (also known as trade-off analysis).

EVALUATION OF ALTERNATIVES

TASK 3-2: Evaluate alternative courses of action for responding to risk.

Once an initial acceptable level of risk has been defined, risk response courses of action should be identified and evaluated for efficacy in enabling the organization to achieve its defined risk threshold. Evaluation of alternatives typically occurs at Levels 1 or 2 with a focus on anticipated organization-wide impacts of C-SCRM to the organization's ability to successfully carry out organizational missions and processes. When carried out at Level 3, evaluation of alternatives will focus on the SDLC or the amount of time available for implementing the course of action.

Each courses of action analyzed may include a combination of risk acceptance, avoidance, mitigation, transfer and/or sharing. For example, an organization may elect to share a portion of its risk to a strategic supplier through the selection of controls included under contractual terms. Alternatively, an organization may choose to mitigate to acceptable levels though the selection and implementation of controls. In many cases, risk strategies will leverage a combination of risk response courses of action.

During evaluation of alternatives, organization will analyze available risk response courses of action for identified cyber supply chain risks. The goal of this exercise is to enable the organization to achieve an appropriate balance among C-SCRM and functionality needs of the organization. As a first step, organizations should ensure risk appetites and tolerances, priorities and tradeoffs, applicable requirements and constraints are reviewed with stakeholders familiar with broader organizational requirements, such as cost, schedule, performance, policy, and compliance. Through this process, the organization will identify risk response implications to the organization's broader requirements. Equipped with a holistic understanding of risk response implications, organizations should perform the C-SCRM, mission, and operational-level trade-off analyses to identify the correct balance of C-SCRM controls to respond to risk. At Level 3, the Frame, Assess, Respond, and Monitor process feeds into the RMF Select step described in [NIST SP 800-37 Rev. 2].

The selected C-SCRM controls for a risk response course of action will vary depending on where they are applied within organizational levels and SDLC processes. For example, C-SCRM controls may range from using a blind buying strategy to obscure end use of a critical component, to design attributes (e.g., input validation, sandboxes, and anti-tamper design). For each implemented control, the organization should identify someone responsible for its execution and develop a time- or event-phased plan for implementation throughout the SDLC. Multiple controls may address a wide range of possible risks. Therefore, understanding how the controls impact the overall risk is essential and must be considered before choosing and tailoring the combination of controls as yet another trade-off analysis may be needed before the controls can be finalized. The organization may be trading one risk for a larger risk unknowingly if the

dependencies between the proposed controls and the overall risk are not well-understood and addressed.

RISK RESPONSE DECISION

TASK 3-3: Decide on the appropriate course of action for responding to risk.

As described in [NIST SP 800-39], organizations should select, tailor, and finalize C-SCRM controls, based on the evaluation of alternatives and an overall understanding of threats, risks, and supply chain priorities. Within Levels 1 and 2, the resulting decision, along with selected and tailored common control baselines (i.e., revisions to established baselines) should be documented within a C-SCRM-specific Risk Response Framework.[36] Within Level 3, the resulting decision, along with the selected and tailored controls, should be documented within the C-SCRM Plan as part of an authorization package.

Risk response decisions may be made by a risk executive or delegated by the risk executive to someone else in the organization. While the decision can be delegated to Level 2 or Level 3, the significance and the reach of the impact should determine the level at which the decision is being made. Risk response decisions may be made in collaboration with an organization's risk executives, mission owners, and system owners, as appropriate. Risk response decisions are heavily influenced by the organization's predetermined appetite and tolerance for risk. Using robust risk appetite and tolerance definitions, decision makers can ensure consistent alignment of the organization's risk decisions with its strategic imperatives. Robust definitions of risk appetite and tolerance may also enable organizations to delegate risk decision responsibility to lower levels of the organization and provide greater autonomy across the Levels.

Within Levels 1 and 2, the resulting decisions should be documented, along with any changes to requirements or selected common control baselines (enterprise or mission level), within C-SCRM-specific Risk Response Frameworks. The C-SCRM Risk Response Framework may influence other related Risk Response Frameworks.

The Risk Response Framework should include:

- Describing the threat source, threat event, exploited vulnerability, and threat event outcome;
- Providing an analysis of the likelihood and impact of the risk and final risk score;
- Describing the selected mitigating strategies and controls along with an estimate of the cost and effectiveness of the mitigation against the risk.

Within Level 3, the resulting decision, along with the selected and tailored controls, should be documented in a C-SCRM Plan. While the C-SCRM Plan is ideally developed proactively, it may also be developed in response to a cyber supply chain compromise. Ultimately, the C-SCRM Plan should cover the full SDLC, document a C-SCRM baseline, and identify cyber

[36] More information can be found on Risk Response Frameworks in Appendix B along with explicit examples.

supply chain requirements and controls at the Level 3 operational-level. The C-SCRM Plan should be revised and updated based on the output of cyber supply chain monitoring.

C-SCRM Plans should:

- Summarize the environment as determined in Frame such as applicable policies, processes, and procedures based on organization and mission requirements currently implemented in the organization;
- State the role responsible for the plan such as Risk Executive, Chief Financial Officer (CFO), Chief Information Officer (CIO), Program Manager, or System Owner;
- Identify key contributors such as CFO, Chief Operations Officer (COO), Acquisition/Contracting, Procurement, C-SCRM PMO, System Engineer, System Security Engineer, Developer/Maintenance Engineer, Operations Manager, or System Architect;
- Provide the applicable (per level) set of risk mitigation measures and controls resulting from the Evaluation of Alternatives (in Respond);
- Provide tailoring decisions for selected controls including the rationale for the decision;
- Describe feedback processes among the levels to ensure that cyber supply chain interdependencies are addressed;
- Describe monitoring and enforcement activities (including auditing if appropriate) applicable to the scope of each specific C-SCRM Plan;
- If appropriate, state qualitative or quantitative measures to support implementation of the C-SCRM Plan and assess effectiveness of this implementation;[37]
- Define frequency for deciding whether the plan needs to be reviewed and revised;
- Include criteria that would trigger revision, for example, life cycle milestones, gate reviews, or significant contracting activities; and
- Include suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers C-SCRM Plans if made available as part of agreements.

Agencies may want to integrate C-SCRM controls into the respective System Security Plans or develop separate operational-level C-SCRM Plans. At Level 3, the C-SCRM Plan applies to High and Moderate Impact systems per [FIPS 199]. Requirements and inputs from the Enterprise C-SCRM strategy at Level 1, and Mission C-SCRM strategy and implementation plan at Level 2, should flow down and be used to guide the develop C-SCRM Plans at Level 3. Conversely, the C-SCRM controls and requirements at Level 3 should be considered in developing and revising requirements and controls applied at the higher levels. C-SCRM Plans should be interconnected and reference each other when appropriate.

Table 2-7 summarizes the controls to be contained in Risk Response Frameworks at Levels 1 and 2, and C-SCRM Plans at Level 3 and provides examples of those controls.

[37] NIST SP 800-55 Revision 1, *Performance Measurement Guide for Information Security* (July 2008), provides guidance on developing information security measures. Agencies can use general guidance in that publication to develop specific measures for their C-SCRM plans. See http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

Table C-9: Controls at Levels 1,2, and 3

Level	Controls	Examples
Level 1	Provides organization common controls baseline to Levels 2 and 3	• Minimum sets of controls applicable to all suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. • Enterprise-level controls applied to processing and storing suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers information. • Cyber supply chain training and awareness for acquirer staff at the enterprise-level.
Level 2	• Inherits common controls from Level 1 • Provides mission and business process0level common controls baseline to Level 3 Provides feedback to Level 1 about what is working and what needs to be changed	• Minimum sets of controls applicable suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers for the specific mission and business process. • Program-level refinement of Identity and Access Management controls to address C-SCRM concerns. • Program-specific supply chain training and awareness.
Level 3	• Inherits common controls from Levels 1 and 2 • Provides system-specific controls for Level 3 Provides feedback to Level 2 and Level 1 about what is working and what needs to be changed	• Minimum sets of controls applicable to service providers or specific hardware and software for the individual system. • Appropriately rigorous acceptance criteria for change management for systems that support supply chain, e.g., as testing or integrated development environments. • System-specific cyber supply chain training and awareness. • Intersections with the SDLC.

Appendix C provides an example C-SCRM Plan template with the sections and types of information organizations should include in their C-SCRM Planning activities.

RISK RESPONSE IMPLEMENTATION

TASK 3-4: Implement the course of action selected to respond to risk.

Organizations should implement the C-SCRM Plan in a manner that integrates the C-SCRM controls into the overall agency risk management processes.

Outputs and Post Conditions

The output of this step is a set of C-SCRM controls that address C-SCRM requirements and can be incorporated into the system requirements baseline and in agreements with third-party providers. These requirements and resulting controls will be incorporated into the SDLC and other organizational processes, throughout the three levels.

For general risk types, this step results in:

- Selected, evaluated, and tailored C-SCRM controls that address identified risks;
- Identified consequences of accepting or not accepting the proposed mitigations; and
- Development and implementation of the C-SCRM Plan.

MONITOR
Inputs and Preconditions

Monitor is the step in which organizations: (i) verify compliance; (ii) determine the ongoing effectiveness of risk response measures; and (iii) identify risk-impacting changes to organizational information systems and environments of operation.

Changes to the organization, mission/business, operations, or the supply chain can directly impact the organization's cyber supply chain. The Monitor step provides a mechanism for tracking such changes and ensuring they are appropriately assessed for impact (in Assess). If the cyber supply chain is redefined as a result of monitoring, organizations should coordinate with the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to resolve implications and mutual obligations.

Organizations should integrate C-SCRM into existing continuous monitoring programs.[38] In the event a Continuous Monitoring program does not exist, C-SCRM can serve as a catalyst for establishing a comprehensive continuous monitoring program. Figure 2-8 depicts the Monitor Step with inputs and outputs along the three organizational levels.

[38] NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (September 2011), describes how to establish and implement a continuous monitoring program. See http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.

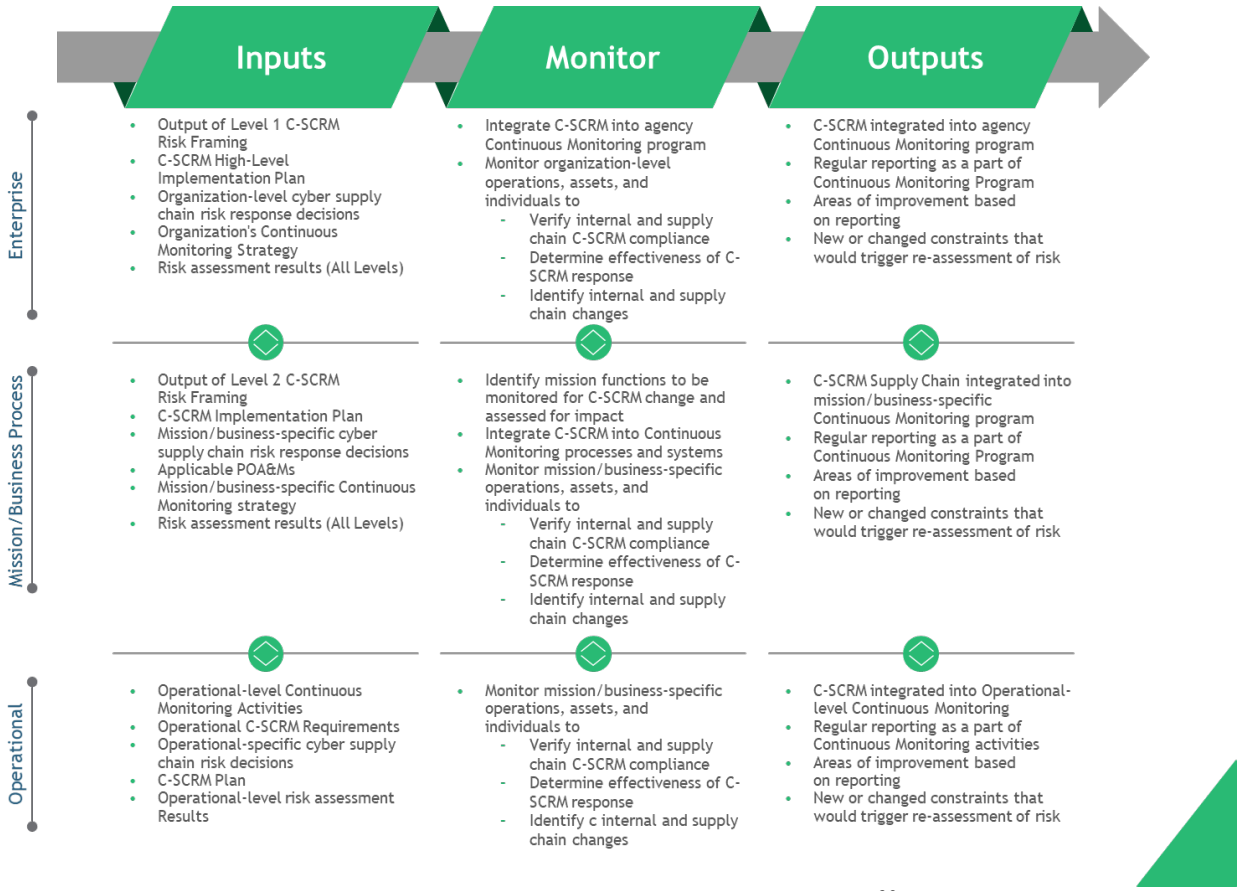


Fig. C-5: C-SCRM in the Monitor Step[39]

Activities

RISK MONITORING STRATEGY

TASK 4-1: Develop a risk monitoring strategy for the organization that includes the purpose, type, and frequency of monitoring activities.

Supplemental Guidance

Organizations should integrate C-SCRM considerations into their overall risk monitoring strategy. Monitoring cyber supply chain risk may require access to information that agencies may not have traditionally collected. Some of the information will require needing to be gathered from outside the agency, such as from open sources or suppliers and integrators. The strategy should, among other things, include the data to be collected, state the specific measures compiled from the data (e.g., number of contractual compliance violations by the vendor), identify existing or include assumptions about required tools needed to collect the data, identify how the data will be protected, and define reporting formats for the data. Potential data sources may include:

- Agency vulnerability management and incident management activities;
- Agency manual reviews;

[39] More detailed information on the Risk Management Process can be found in Appendix C

- Interagency information sharing;
- Information sharing between the agency and suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers;
- Supplier information sharing; and
- Contractual reviews of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

Organizations should ensure the appropriate protection of supplier data if that data is collected and stored by the agency. Agencies may also require additional data collection and analysis tools to appropriately evaluate the data to achieve the objective of monitoring applicable cyber supply chain risks.

RISK MONITORING

TASK 4-2: Monitor organizational information systems and environments of operation on an ongoing basis to verify compliance, determine effectiveness of risk response measures, and identify changes.

According to [NIST SP 800-39], organizations should monitor compliance, effectiveness, and change. Monitoring compliance within the context of C-SCRM involves monitoring an organization's processes and supplied products and services for compliance with the established security and C-SCRM requirements. Monitoring effectiveness involves monitoring the resulting risks to determine whether these established security and C-SCRM requirements produce the intended results. Monitoring change involves monitoring the environment for any changes that would signal changing requirements and mitigations/controls to maintain an acceptable level of cyber supply chain risk.

To monitor changes, organizations need to identify and document the set of triggers that would change cyber supply chain risk. While the categories of triggers will likely include changes to constraints, identified in Table 2-6 (during the Frame Step), such as policy, mission, change to the threat environment, enterprise architecture, SDLC, or requirements, the specific triggers within those categories may be substantially different for different organizations.

An example of a cyber supply chain change is two key vetted suppliers[40] announcing their departure from a specific market, therefore creating a supply shortage for specific components. This would trigger the need to evaluate whether reducing the number of suppliers could create vulnerabilities in component availability and integrity. In this scenario, potential deficit of components may result simply from insufficient supply of components, because fewer components are available. If none of the remaining suppliers are vetted, this deficit may result in uncertain integrity of the remaining components. If the organizational policy directs use of vetted components, this event may result in the organization's inability to fulfill its mission needs.

[40] A vetted supplier is a supplier with whom the organization is comfortable doing business. This level of comfort is usually achieved through developing an organization-defined set of supply chain criteria and then *vetting* suppliers against those criteria.

In addition to regularly updating existing risks assessments with the results of the ongoing monitoring, the organization should determine the triggers of a reassessment. Some of these triggers may include availability of resources, changes to cyber supply chain risk, natural disasters, or mission collapse.

Outputs and Post Conditions

Organizations should integrate the cyber supply chain outputs of the Monitor Step into the C-SCRM Plan. This plan will provide inputs into iterative implementations of the Frame, Assess, and Respond Steps as required.

APPENDIX D: C-SCRM TEMPLATES

1. C-SCRM STRATEGY & IMPLEMENTATION PLAN

To address supply chain risks, organizations develop a C-SCRM strategy. The C-SCRM strategy, accompanied by an implementation plan, is at the enterprise level (Level1), though different mission/business areas (Level 2) may further tailor the C-SCRM strategy to address specific mission/business needs as outlined at the organizational level. The C-SCRM strategy and implementation plan should anchor to the overarching enterprise risk management strategy and comply with applicable laws, executive orders, directives, and regulations.

Typical components of the strategy and implementation plan, as outlined in the below template, include strategic approaches to reducing an organization's supply chain risk exposure via enterprise-wide risk management requirements, ownership, risk tolerance, roles and responsibilities, and escalation criteria.

1.1. C-SCRM Strategy & Implementation Plan Template

1.1.1. Purpose

Outline the organization's high-level purpose for the strategy and implementation document, aligning that purpose to organizational mission, vision, and values. Describe where the strategy and implementation document resides relative to other C-SCRM documentation that must be maintained at various tiers. Provide clear direction around the organization's C-SCRM priorities and its general approach for achieving those priorities.

Sample Text

The purpose of this strategy and implementation document is to provide a strategic roadmap for implementing effective C-SCRM capabilities, practices, processes, and tools within the organization and in support of its vision, mission, and values.

The strategic approach is organized around a set of objectives that span the scope of the organization's mission and reflect a phased, achievable strategic approach to ensure successful implementation and effectiveness of C-SCRM efforts across the enterprise.

This strategy and implementation document discusses the necessary core functions, roles, and responsibilities, and the approach the organization will take to implement C-SCRM capabilities within the enterprise. As mission/business policies and system plans are developed and completed, they will be incorporated as attachments to this document. All three tiers of documentation should be periodically reviewed together to ensure cohesion and consistency.

The focus of this strategy and implementation plan is intentionally targeted toward establishing a core foundational capability. These baseline functions, such as defining policies, ownership, and dedicated resources will ensure the organization can expand and mature its C-SCRM capabilities over time. This plan also acknowledges and emphasizes the need to raise awareness and ensure training for staff in order to understand C-SCRM and grow the competencies necessary to be able to perform C-SCRM functions.

This initial strategy and implementation plan also recognizes the dependencies on industry-wide coordination efforts, processes, and decisions. As government and industry-wide direction, process guidance, and requirements are clarified and communicated, the organization will update and refine its strategy and operational implementation plans and actions.

1.1.2. Authority & Compliance

List of the laws, executive orders, directives, regulations, policies, standards, and guidelines that govern C-SCRM Strategy and Implementation.

Sample Text

- Legislation
  - Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology of 2018
  - Federal Information Security Modernization Act of 2014
  - Section 889 of the 2019 National Defense Authorization Act - "Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment"
  - Gramm-Leach-Bliley Act
  - Health Insurance Portability and Accountability Act
- Regulations
  - NYDFS 23 NYCRR 500: Section 500.11 Third Party Service Provider Security Policy
  - CIP-013-1: Cyber Security - Supply Chain Risk Management
  - FFIEC Information Security Handbook II.C.20: Oversight of Third-Party Service Providers
- Guidelines
  - NIST 800-53 Revision 5: CA-5, SR-1, SR-2, SR-3
  - NIST 800-37 Revision 2
  - NIST 800-161 Revision 1: Appendix C
  - ISO 28000:2007

1.1.3. Strategic Objectives

Strategic objectives establish the foundation for determining enterprise-level C-SCRM controls and requirements. Each objective supports achievement of the organization's stated purpose in pursuing sound C-SCRM practices and risk-reducing outcomes. Together, the objectives provide the organization with the essential elements needed to bring C-SCRM capabilities to life, and effectively pursue the organization's purpose.

In aggregate, strategic objectives should address essential C-SCRM capabilities and enablers, such as:

- Implementing a risk management hierarchy and risk management approach;
- Establishing an organization governance structure that integrates C-SCRM requirements and incorporates these requirements into organizational policies;
- Defining a supplier risk assessment approach;

- Implementing a quality and reliability program that includes quality assurance and quality control process and practices;
- Establishing explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, and physical security (and other relevant) functions;
- Ensuring that adequate resources are dedicated and allocated to information security and C-SCRM to ensure proper implementation of policy, guidance, and controls;
- Implementing a robust incident management program to successfully identify, respond to, and mitigate security incidents; and
- Including key suppliers in contingency planning, incident response, and disaster recovery planning and testing.

Sample Text

Objective 1: Effectively manage cyber supply chain risks

This objective addresses the primary intent of the organization's pursuit of C-SCRM. The establishment and sustainment of an enterprise-wide C-SCRM program will enable the organization's risk owners to identify, assess, and mitigate supply chain risk to the organization's assets, functions, and associated services. Implementing an initial capability that can sustain and grow in its scope of focus and breadth and depth of functions will be done in phases and will consider holistic "people, process, and technology" needs to ensure the organization is able to achieve desired C-SCRM goals in areas such as improving enterprise awareness, protection, and resilience.

Objective 2: Serve as a trusted source of supply for customers

Addressing customer supply chain risks at scale and across the organization's diverse portfolio demands a prioritization approach, structure, improved processes, and ongoing governance. C-SCRM practices and controls need to be tailored to address the distinct and varied supply chain threats and vulnerabilities that are applicable for the organization's customers. This objective can be achieved by:

- Strengthening vetting processes, C-SCRM requirements, and oversight of external providers;
- Ensuring customer needs are met in line with their cyber supply chain risk appetite, tolerance, and environment.

Objective 3: Position as an industry leader in C-SCRM

The organization is well-positioned to enable and drive improvements forward in addressing how cyber supply chain risks across the industry. Therefore, we must use this position to advocate with industry stakeholders about communication, incentivization, and education of industry players about our requirements and expectations related to addressing supply chain risk.

1.1.4. Implementation Plan & Progress Tracking

Outline the methodology and milestones by which progress against the enterprise's C-SCRM strategic objectives will be tracked. Though organizational context heavily informs this process, organizations should define prioritized time horizons to encourage execution of tasks critical or foundational in nature. Common nomenclature for defining such time horizons includes "crawl, walk, run" or "do now, do next, do later." Regardless of the time horizon designated, implementation of practical, prioritized plans is essential to building momentum in the establishment or enhancement of C-SCRM capabilities.

Once the implementation plan is baselined, an issue escalation process and feedback mechanism is included that drives changes to the implementation plan and progress tracking.

Sample Text

[Organization's] execution of its C-SCRM strategic objectives and sustained operational effectiveness of underlying activities requires a formal approach and commitment to progress tracking. [Organization] will track and assess implementation of its strategic objectives by defining subsidiary milestones and implementation dates in an implementation plan. Monitoring and reporting against implementation plan requires shared responsibility across multiple disciplines and requires a cross-organization, team-based approach.

The following implementation plan will be continuously maintained by mission/business owners and reviewed by the Senior Leadership team as a part of regular oversight activities.

Risks and issues impacting the implementation plan should be raised proactively by mission/business owners, or their team, to the Senior Leadership Team. The implementation plan may then be revised in accordance with Senior Leadership Team's discretion.

Objective 1: Effectively manage cyber supply chain risks				
Implementation Plan Milestone	Status	Owner	Priority	Target Date
Establish policy and authority	Planned	J. Doe	Do Now	XX/XX/XX
Establish and provide executive oversight and direction	Complete	…	Do Next	…
Integrate C-SCRM into enterprise risk management (ERM) framework	Delayed	…	Do Later	…
Establish C-SCRM PMO capability and organization	Cancelled	…	…	…
Establish roles, responsibilities, and assign accountability	…	…	…	…
Develop C-SCRM plans	…	…	…	…
Stand up internal awareness function	…	…	…	…

Identify, prioritize, and implement supply chain risk assessment capabilities	…	…	…	…
Establish, document, and implement enterprise-level C-SCRM controls	…	…	…	…
Identify C-SCRM resource requirements and secure sustained funding	…	…	…	…
Establish C-SCRM program performance monitoring	…	…	…	…

7635

Objective 2: Serve as a trusted source of supply for customers				
Implementation Plan Milestone	Status	Owner	Priority	Target Date
Incorporate C-SCRM activities customer-facing business lines, programs, and solution offerings	Planned	J. Doe	Do Now	XX/XX/XX
Ensure customer support personnel are well versed in cyber supply chain risks and management requirements	Complete	…	Do Next	…
Establish minimum baseline levels of cyber supply chain assurance	Delayed	…	Do Later	…
Establish processes to respond to identified risks and to monitor for impacts to the organization's cyber supply chain	Cancelled	…	…	…

7636

Objective 3: Position as an industry leader in C-SCRM				
Implementation Plan Milestone	Status	Owner	Priority	Target Date
Coordinate and engage with national security and law enforcement to ensure rapid access to mission-critical supply chain threats	Planned	J. Doe	Do Now	XX/XX/XX
Evaluate C-SCRM improvement opportunities and strengthen requirements and oversight for industry-wide common solutions / shared services	Complete	…	Do Next	…
Advocate for C-SCRM awareness and competency through training and workforce development	Delayed	…	Do Later	…
Release whitepapers and public guidance related to C-SCRM	Cancelled	…	…	…

1.1.5. Roles & Responsibilities

Assign those responsible for the Strategy & Implementation template, as well as its key contributors. Include the role and name of each individual or group, as well contact information where necessary (e.g., organizational affiliation, address, email address, and phone number).

Sample Text

- Senior Leadership Team shall:
  - endorse the enterprise's C-SCRM strategic objectives and implementation plan
  - provide oversight of C-SCRM implementation and effectiveness
  - communicate C-SCRM direction and decisions for priorities and resourcing needs
  - determine the enterprise's risk appetite and risk tolerance; and
  - respond to high-risk C-SCRM issue escalations that could impact the organization's risk posture in a timely manner.

- Mission/Business Owners shall:
  - determine mission level risk appetite and tolerance, ensuring they are in line with enterprise expectations
  - define supply chain risk management requirements and implementation of controls that support enterprise objectives
  - maintain criticality analyses of mission functions and assets; and
  - perform risk assessments for mission/business-related procurements.

1.1.6. Definitions

List the key definitions described within the Strategy & Implementation template, providing organizationally specific context and examples where needed.

Sample Text

- Enterprise: An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information, and mission management.

- Objective: An organization's broad expression of goals. Specified target outcome for operations.

1.1.7. Revision & Maintenance

Define the required frequency of Strategy & Implementation template revisions. Maintain a table of revisions to enforce version control. Strategy & Implementation templates are living documents that must be updated and communicated to all appropriate individuals (e.g., staff, contractors, and suppliers).

Sample Text

[Organization's] Strategy & Implementation template must be reviewed at a minimum every 3-5 years (within the federal environment) since changes to laws, policies, standards, guidelines, and controls are dynamic and evolving. Additional criteria that may trigger interim revisions include:

- change of policies that impact the Strategy & Implementation template;
- significant Strategy & Implementation events;
- introduction of new technologies;
- discovery of new vulnerabilities;
- operational or environmental changes;
- shortcomings in the Strategy & Implementation template;
- change of scope; and
- other organization-specific criteria.

Sample Version Management Table

Version Number	Date	Description of Change/Revision	Section/Pages Affected	Changes made by Name/Title/Organization

2. C-SCRM POLICY

The C-SCRM policies direct the implementation of the C-SCRM strategy. C-SCRM policies can be developed at Level 1 and/or at Level 2 and are informed by the mission/business specific factors, including risk context, risk decisions and risk activities from the C-SCRM strategy. The C-SCRM policies support applicable organizational policies (e.g., acquisition and procurement, information security and privacy, logistics, quality, and supply chain). The C-SCRM policies address the goals and objectives outlined in the organization's C-SCRM strategy, which in turn is informed by the organization's strategic plan. The C-SCRM policies should also address missions and business functions, and the internal and external customer requirements. C-SCRM policies also define the integration points for C-SCRM with the risk management and processes for the organization. Finally, the C-SCRM policies define at a more specific and granular level the C-SCRM roles and responsibilities within the organization, any interdependencies among those roles, and the interaction among the roles; the C-SCRM policies at Level 1 are more broad-based, whereas the C-SCRM policies at Level 2 are specific to the mission/business function. C-SCRM roles specify the responsibilities for procurement, conducting risk assessments, collecting supply chain threat intelligence, identifying and implementing risk-based mitigations, performing monitoring, and other C-SCRM functions.

2.1. C-SCRM Policy Template

2.1.1. Authority & Compliance

List of the laws, executive orders, directives, regulations, policies, standards, and guidelines that govern the C-SCRM policy.

Sample Level 1 Text

- Policies
  - [Organization Name] Enterprise Risk Management Policy
  - [Organization Name] Information Security Policy
- Legislation
  - Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology of 2018
- Regulations
  - NYDFS 23 NYCRR 500: Section 500.11 Third Party Service Provider Security Policy
  - CIP-013-1: Cyber Security - Supply Chain Risk Management
  - FFIEC Information Security Handbook II.C.20: Oversight of Third-Party Service Providers

Sample Level 2 Text

- Policies
  - [Organization Name] C-SCRM Policy

7741 - [Mission and Business Process Name] Information Security Policy
7742 - Regulations
7743 - NYDFS 23 NYCRR 500: Section 500.11 Third Party Service Provider Security
7744 Policy
7745 - Guidelines
7746 - NIST 800-53 Revision 5: SR-1, PM-9, PM-30, PS-8, SI-12
7747 - NIST 800-161 Revision 1: Appendix C
7748

7749 **2.1.2. Description**

7750

7751 *Describe the purpose and scope of the C-SCRM policy, outlining the organizational leaderships'*
7752 *intent to adhere to the plan, enforce its controls, and ensure that it remains current. Define the*
7753 *tier(s) at which the policy applies. C-SCRM policies may need to be derived in whole or in part*
7754 *from existing policies or other guidance.*
7755

7756 *For Level 2 C-SCRM policies should list all Level 1 policies and plans that inform the Level 2*
7757 *policies, provide a brief explanation of what this mission/business encompasses and briefly*
7758 *describe the scope of applicability (e.g. plans, systems, type of procurements, etc.) for these*
7759 *Level 2 C-SCRM policies.*
7760

7761 **Sample Level 1 Text**

7762

7763 [Organization] is concerned about the risks in the products, services, and solutions bought, used,
7764 and offered to customers.
7765

7766 The policy objective of the [Organization's] C-SCRM Program is to successfully implement and
7767 sustain the capability of providing improved assurance that the products, services, and solutions
7768 used and offered by [Organization] are trustworthy, appropriately secure and resilient, and able
7769 to perform to the required quality standard.
7770

7771 C-SCRM is a systematic process for identifying and assessing susceptibilities, vulnerabilities,
7772 and threats throughout the supply chain and implementing strategies and mitigation controls to
7773 reduce risk exposure and combat threats. The establishment and sustainment of an enterprise-
7774 wide C-SCRM Program will enable [Organization's] risk owner(s) to identify, assess, and
7775 mitigate supply chain risk to [Organization's] mission assets, functions, and associated services.
7776

7777 **Sample Level 2 Text**

7778

7779 [Mission and Business Process] recognizes its criticality to [Organization Objective]. A key
7780 component of producing products involves coordinating among multiple suppliers, developers,
7781 system integrators, external system service providers, and other ICT/OT-related service
7782 providers. [Mission and Business Process] understands the realization of cyber supply chain risks
7783 may disrupt or completely inhibit [Mission and Business Process]'s ability to generate products
7784 in a timely manner and in accordance with the required quality standard.
7785

Based on the C-SCRM objectives set forth by [Organization Level 1 Policy Name], [Mission and Business Process]'s policy objective is to implement C-SCRM capabilities allowing for the assessment, response, and monitoring of cyber supply chain risks. C-SCRM capabilities that align with the policy and requirements set forth by the enterprise-wide C-SCRM program will provide the boundaries within which [Mission and Business Process Name] will tailor C-SCRM processes and practices to meet the unique requirements associated with sourcing components and assembling key products.

2.1.3. Policy

Outline the mandatory high-level policy statements that underpin the goals and objectives of the C-SCRM organization's strategic plan, missions and business functions, and the internal and external customer requirements.

Sample Level 1 Text

[Organization's] enterprise-level C-SCRM Program is established to implement and sustain the capability to:

- assess and provide appropriate risk response to cyber supply chain risk posed by the acquisition and use of covered articles;
- prioritize cyber supply chain risk assessments and risk response actions based on criticality assessment of mission, system, component, service, or asset;
- develop an overall C-SCRM strategy and high-level implementation plan and policies and processes;
- integrate supply chain risk management practices throughout the acquisition and asset management life cycle of covered articles;
- share C-SCRM information in accordance with industry-wide criteria and guidelines; and
- guide and oversee implementation progress and program effectiveness.

The C-SCRM Program shall:

- be centrally led and coordinated by a designated senior leadership who shall function as the [Organization's] C-SCRM Program Executive and chair the C-SCRM Program Management Office (PMO);
- leverage and be appropriately integrated into existing [Organization's] risk-management and decision-making governance processes and structures;
- reflect a team-based approach and be collaborative, interdisciplinary, and intra-organizational in nature and composition;
- incorporate a Leveled risk management approach, consistent with the NIST Risk Management Framework and NIST's supply chain risk management Special Publication 800-161 Revision 1; and
- implement codified and regulatory C-SCRM requirements and industry-wide and [Organization]-specific policy direction, guidance, and processes.

Sample Level 2 Text

[Mission and Business Process]'s C-SCRM Program shall:

- operate in accordance with requirements and guidance set forth by [Organization] C-SCRM Program
- collaborate with the C-SCRM Program Management Office (PMO) to apply C-SCRM practices and capabilities needed to assess, respond to, and monitor cyber supply chain risk arising from pursuit of [Mission and Business Process]'s core objectives
- integrate C-SCRM activities into applicable activities to support [Organization]'s objective to manage cyber supply chain risk
- assign and dedicate resources responsible for coordinating C-SCRM activities within [Mission and Business Process]
- identify [Mission and Business Process]'s critical suppliers and assess level of risk exposure that arises as a result of that relationship
- implement risk response efforts to reduce exposure to cyber supply chain risk
- monitor [Mission and Business Process]'s ongoing exposure cyber supply chain risk profile and provide periodic reporting to identified [Organization] enterprise risk management and C-SCRM stakeholders

2.1.4. Roles & Responsibilities

State those responsible for the C-SCRM policies, as well as its key contributors. Include the role and name of each individual or group, as well contact information where necessary (e.g., organizational affiliation, address, email address, and phone number).

Sample Level 1 Text

- The C-SCRM Program Executive shall be responsible for:
  - leading the establishment, development, and oversight of the C-SCRM Program, in coordination and consultation with designated C-SCRM Leads;
  - establishing and serving as the Chair of the C-SCRM PMO. This Team will be comprised of the chair and the designated C-SCRM Leads and will be responsible for developing and coordinating C-SCRM strategy and implementation plans and actions, addressing C-SCRM-related issues, program reporting and oversight, and identifying and making program resource recommendations; and
  - escalating and/or reporting C-SCRM issues to Senior Officials, as may be appropriate.

- Each C-SCRM Security Officer shall be responsible for:
  - identify C-SCRM Leads (the Lead will be responsible for participating as a collaborative and core member of the C-SCRM PMO);
  - incorporate relevant C-SCRM functions into organization and position-level functions; and
  - implement and conform to C-SCRM Program requirements

Sample Level 2 Text

- C-SCRM Leads shall be responsible for:

7874 - representing the interests and needs of C-SCRM PMO members; and
7875 - leading and/or coordinating the development and execution of program or
7876 business-line C-SCRM plan(s). This shall include ensuring such plan(s) are
7877 appropriately aligned to and integrated with the enterprise-level C-SCRM plan.
7878
7879 • Mission and Business Process C-SCRM Staff shall be responsible for:
7880 - Primary execution of C-SCRM activities (e.g., supplier or product assessments)
7881 - Support mission and business-specific C-SCRM activities driven by non-C-
7882 SCRM staff
7883

7884 **2.1.5. Definitions**
7885
7886 *List the key definitions described within the policy, providing organizationally-specific context*
7887 *and examples where needed.*
7888
7889 **Sample Text (Applies to Level 1 and/or Level 2)**

7890 • Covered Articles: Information technology, including cloud computing services of all
7891 types; Telecommunications equipment or telecommunications service; the processing of
7892 information on a Federal or non-Federal information system, subject to the requirements
7893 of the Controlled Unclassified Information program; all IoT/OT - (hardware, systems,
7894 devices, software, or services that include embedded or incidental information
7895 technology.

7896 • Cyber Supply Chain Risk Assessment: Cyber Supply Chain Risk Assessment is a
7897 systematic examination of cyber supply chain risks, likelihoods of their occurrence, and
7898 potential impacts.

7899 • Risk Owner: A person or entity with the accountability and authority to manage a risk.

7900

7901 **2.1.6. Revision & Maintenance**
7902
7903 *Define the required frequency for the C-SCRM policy. Maintain a table of revisions to enforce*
7904 *version control. C-SCRM policies are living documents that must be updated and communicated*
7905 *to all appropriate individuals (e.g., staff, contractors, and suppliers).*
7906
7907 **Sample Text (Applies to Level 1 and/or Level 2)**
7908
7909 [Organization's] C-SCRM policy must be reviewed at a minimum on an annual basis since
7910 changes to laws, policies, standards, guidelines, and controls are dynamic and evolving.
7911 Additional criteria that may trigger interim revisions include:

7912 • change of policies that impact the C-SCRM policy;
7913 • significant C-SCRM events;
7914 • introduction of new technologies;
7915 • discovery of new vulnerabilities;

- operational or environmental changes;
- shortcomings in the C-SCRM policy;
- change of scope; and
- other organization-specific criteria.

Sample Version Management Table

Version Number	Date	Description of Change/Revision	Section/Pages Affected	Changes made by Name/Title/Organization

3. C-SCRM PLAN

The C-SCRM plan is developed at Tier 3 and is implementation specific, providing policy implementation, requirements, constraints, and implications. It can either be stand-alone or components may be incorporated into system security and privacy plans. The C-SCRM plan addresses managing, implementation, and monitoring of C-SCRM controls and the development/sustainment of systems across the SDLC to support mission and business functions. The C-SCRM Plan applies to High and Moderate Impact systems per [FIPS 199].

Given cyber supply chains can differ significantly across and within organizations, C-SCRM plans should be tailored to the individual program, organizational, and operational contexts. Tailored C-SCRM plans provide the basis for determining whether a technology, service, system component, or system is fit for purpose, and as such, the controls need to be tailored accordingly. Tailored C-SCRM plans help organizations focus their resources on the most critical mission and business functions based on mission and business requirements and their risk environment.

The following C-SCRM Plan template is provided only as an example. Organizations have the flexibility to develop and implement various approaches for the development and presentation of the C-SCRM plan. Organizations can leverage automated tools to ensure all relevant sections of the C-SCRM plan are captured. Automated tools can help document C-SCRM plan information such as component inventories, individuals filling roles, security control implementation information, system diagrams, supply chain component criticality, and interdependencies.

3.1. C-SCRM Plan Template

3.1.1. System Name & Identifier

Designate a unique identifier and/or name for the system. Include any applicable historical names and relevant Tier 1 and Tier 2 document titles.

Sample Text

This C-SCRM Plan provides an overview of the security requirements for the [SYSTEM NAME] [UNIQUE IDENTIFIER] and describes the cyber supply chain controls in place or planned for implementation to provide fit for purpose C-SCRM controls appropriate for the information to be transmitted, processed or stored by the system.

The security safeguards implemented for the [UNIQUE IDENTIFIER] meet the requirements set forth in the organization's C-SCRM strategy and policy guidance.

3.1.2. System Description

Describe the function, purpose, and scope of the system and include a description of the information processed. Provide a general description of the system's approach to 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.

Ensure the C-SCRM plan describes the system in the context of the organization's supply chain risk tolerance, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the plan, and a description of and justification for supply chain risk mitigation measures taken. Descriptions must be consistent with the high-level mission/business function of the system, the authorization boundary of the system, overall system architecture, including any supporting systems and relationships, how the system supports organizational missions, and the system environment (e.g., standalone, managed/enterprise, custom/specialized security-limited functionality, cloud) established in Level 1 and 2.

Sample Text

The [Organization's] document management system (DMS) serves to provide dynamic information repositories, file hierarchies, and collaboration functionality to streamline internal team communication and coordination. The data managed within the system contains personally identifiable information (PII). The DMS is a commercial off-the-shelf (COTS) solution that was purchased directly from a verified supplier [Insert Supplier's name] within the United States. It has been functionally configured to meet the organization's needs; no third-party code libraries are utilized to deploy or maintain the system. It is hosted within the management layer of the organization's primary virtual private cloud provider.

The DMS is a Category 1 system, mandating a recovery time objective (RTO) of one hour in the event of downtime. The organization maintains a disaster recovery environment with a second private cloud provider that the organization can cutover to if the Category 1 RTO is not likely to be met on the primary platform.

3.1.3. System Information Type & Categorization

The following tables specify the information types that are processed, stored, or transmitted by the system and/or its in-boundary cyber supply chain. Organizations utilize NIST [SP 800-60 v2], [NARA CUI], or other organization-specific information types to identify information types and provisional impact levels. Using guidance with regard to the categorization of federal information and systems in [FIPS 199], the organization determines the security impact levels for each information type. For each security objective (i.e., confidentiality, integrity, availability), provide the impact level (i.e., low, moderate, high).

Sample Text

Information Type	Security Objectives		
	Confidentiality (Low, Moderate, High)	Integrity (Low, Moderate, High)	Availability (Low, Moderate, High)

Based on the table above, indicate the high-water mark for each of the security impacts (i.e., low, moderate, high). Determine the overall system categorization.

Security Objective	Security Impact Level
Confidentiality	☐ Low ☐ Moderate ☐ High
Integrity	☐ Low ☐ Moderate ☐ High
Availability	☐ Low ☐ Moderate ☐ High
Overall System Security Categorization	☐ **Low** ☐ **Moderate** ☐ **High**

3.1.4. System Operational Status

Sample Text

Indicate the operational status of the system. If more than one status is selected, list which part of the system is covered under each status

System Status		
☐	Operational	The system is currently operating and is in production.
☐	Under Development	The system is being designed, developed, or implemented
☐	Major Modification	The system is undergoing a major change, development, or transition.
☐	Disposition	The system is no longer operational.

3.1.5. System/Network Diagrams, Inventory, & Lifecycle Activities

Include a current and detailed system and network diagram including a system component inventory or reference to where diagrams and inventory information can be found.

Contextualize the above components against the system's SDLC to ensure activities are mapped and tracked. This ensures full coverage of C-SCRM activities since these activities may require repeating and reintegrating (using spiral or agile techniques) throughout the lifecycle. C-SCRM plan activities are required from concept, all the way through development, production, utilization, support, and retirement steps.

Sample Text

[SYSTEM NAME] components may include:

- Component description
- Version number
- License number
- License holder
- License type (e.g., single user, public license, freeware)
- Barcode/property number
- Hostname (i.e., the name used to identify the component on a network)
- Component type (e.g., server, router, workstation, switch)
- Manufacturer
- Model
- Serial number
- Component revision number (e.g., firmware version)
- Physical location: (include specific rack location for components in computer/server rooms)
- Vendor name(s)

3.1.6. Information Exchange & System Connections

List any information exchange agreements (e.g., Interconnection Security Agreements (ISA), Memoranda of Understanding (MOU), Memoranda of Agreement (MOA)) between the system and another system, date of the agreement, security authorization status of the other system(s), and the name of the authorizing official, provide a description of the connection, and include any diagrams showing the flow of any information exchange.

Sample Text

Agreement Date	Name of System	Organization	Type of Connection or Information Exchange Method	FIPS 199 Categorization	Authorization Status	Authorization Official Name and Title

3.1.7. Security Control Details

Document C-SCRM controls to ensure the plan addresses requirements for developing trustworthy, secure, privacy-protective, and resilient system components and systems, including the application of the security design principles implemented as part of life cycle-based systems security engineering processes. Consider relevant topic areas such as assessments, standard operating procedures, responsibilities, software, hardware, product, service, and DevSecOps considerations.

For each control, provide a thorough description of how the security controls in the applicable baseline are implemented. Include any relevant artifacts for control implementation. Incorporate any control-tailoring justification, as needed. Reference applicable Level 1 and/or Level 2 C-SCRM policies that provide inherited controls where applicable. There may be multiple Level 1 policies that come from the CIO, CAO, or PMO.

Sample Text

SR-6 SUPPLIER ASSESSMENTS AND REVIEWS

Implementation: As a part of a comprehensive, defense-in-breadth information security strategy, the organization established a C-SCRM program to address the management of cyber supply chain risks. The C-SCRM PMO is responsible for conducting cyber supply chain risk assessment (SCRA) for business partners seeking to integrate with [SYSTEM NAME] in accordance with enterprise-wide C-SCRM Level 2 policy requirements. C-SCRM training and awareness materials must also be provided for all individuals prior to receiving access to [SYSTEM NAME].

Control Enhancements: Control enhancements 2, 7 and 8 from NIST 800-161 are applicable.

(2) SUPPLIER REVIEWS
Implementation: C-SCRM PMO provides supplier reviews to business partners in the form of SCRAs before entering into a contractual agreement to acquire information systems, components, or services in relation to [SYSTEM NAME]. The Level 1 strategy and Level 2 policy documents place SCRA requirements on business partners seeking to acquire IT systems,

components, and/or services. The SCRA provides a step-by-step guide for business partners to follow in preparing for an assessment of suppliers by the C-SCRM PMO.

(7) ASSESSMENT PRIOR TO SELECTION/ACCEPTANCE/UPDATE
Implementation: The Level 2 policy defines what [SYSTEM NAME] integration activities require an SCRA. The process and requirements are defined in the SCRA Standard Operating Procedure.

(8) USE OF ALL-SOURCE INTELLIGENCE
Implementation: The C-SCRM PMO utilizes all-source intelligence when conducting supply chain risk assessments for [SYSTEM NAME].

3.1.8. Role Identification

Identify the role, name, department/division, primary and alternate phone number, email address of key cyber supply chain personnel or designate contacts (e.g., vendor contacts, acquisitions subject matter experts (SME), engineering leads, business partners, service providers), with role, name, address, primary and alternate phone numbers, and email address.

Sample Text

Role	Name	Department/ Division	Primary Phone Number	Alternate Phone Number	Email Address
Vendor Contact					
Acquisitions SME					
Engineering Lead					
Business Partner					
Service Provider					

3.1.9. Contingencies & Emergencies

In the event of contingency or emergency operations, organizations may need to bypass normal acquisition processes to allow for mission continuity. Contracting activities that are not vetted using approved C-SCRM plan processes introduce operational risks to the organization. Where appropriate, describe abbreviated acquisition procedures to follow during contingencies and emergencies, such as the contact information for C-SCRM, acquisitions, and legal subject matter experts who can provide advice absent a formal tasking and approval chain of command.

Sample Text

In the event of an emergency where equipment is urgently needed, the C-SCRM PMO will offer its assistance through C-SCRM Subject Matter Experts (SMEs) to provide help in the absence of the formal tasking and chain of command approval. The CIO has the authority to provide such waivers to bypass normal procedures. The current contact information for C-SCRM SMEs is provided below:

- C-SCRM SME POC
  - Name
  - Email
  - Phone
- Acquisitions SME POC
  - Name
  - Email
  - Phone
- Legal SME POC
  - Name
  - Email
  - Phone

3.1.10. Related Laws, Regulations, & Policies

List any applicable laws, executive orders, directives, policies, and regulations that are applicable to the system. For Level 3, include applicable Level 1 C-SCRM Strategy and Implementation Plans and Level 2 C-SCRM Policy titles.

Sample Text

The organization shall ensure that C-SCRM plan controls are consistent with applicable statutory authority, including the Federal Information Security Modernization Act (FISMA); with regulatory requirements and external guidance, including Office of Management and Budget (OMB) policy and Federal Information Processing Standards (FIPS) publications promulgated by the National Institute of Standards and Technology (NIST); and with internal C-SCRM policies and strategy documents.

The following references apply:

- Committee on National Security Systems. CNSSD No. 505. *(U) Supply Chain Risk Management (SCRM)*
- NIST SP 800-53 Revisions 5 *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-161 Revision 1 *Supply Chain Risk Management Practices for Information Systems and Organizations*
- OMB Circular A-130 *Managing Information as a Strategic Resource*
- Federal Acquisition Supply Chain Security Act of 2018

3.1.11. Revision & Maintenance

Include a table identifying the date of the change, a description of the modification, and the name of the individual who made the change. At a minimum, review and update Level 3 C-SCRM plans at life cycle milestones, gate reviews, and significant contracting activities, and verify for compliance with upper tier plans as appropriate. Ensure the plan adapts to shifting impacts of exogenous factors, such as threats, organizational, and environmental changes.

Sample Text

Version Number	Date	Description of Change/Revision	Section/Pages Affected	Changes made by Name/Title/Organization

3.1.12. C-SCRM Plan Approval

Include a signature (either electronic or handwritten) and date when the system security plan is reviewed and approved.

Sample Text

Authorizing Official:

X _____

Name

Date

3.1.13. Acronym List

Include and detail any acronyms utilized in the C-SCRM plan.

Sample Text

Acronym	Detail
AO	Authorizing Official
C-SCRM	Cyber Supply Chain Risk Management
SDLC	System Development Life Cycle

3.1.14. Attachments

Attach any relevant artifacts that can be included to support the C-SCRM plan.

Sample Text

- Contractual agreements
- Contractors' or suppliers' C-SCRM plans

4. CYBER SUPPLY CHAIN RISK ASSESSMENT

The Cyber Supply Chain Risk Assessment (C-SCRA) guides the review of any third-party product, service, or supplier[41] that could present a cyber supply chain risk to a procurer. The objective of the C-SCRA template is to provide a toolbox of questions that an acquirer can choose to use or not use depending on the controls selected. Typically executed by C-SCRM PMOs at the operational level (Level 3), the C-SCRA takes into account available public and private information to perform a holistic assessment, including known cyber supply chain risks, likelihoods of their occurrence, and potential impacts to an organization and its information and systems. As organizations may be inundated with C-SCRAs, and suppliers inundated with C-SCRA requests, the organization should evaluate the relative priority of its C-SCRAs as an influencing factor on the rigor of the C-SCRA.

As with the other featured templates, the below C-SCRA is provided only as an example. Organizations must tailor the below content to align with their Level 1 and 2 risk postures. The execution of C-SCRAs is perhaps the most visible and time-consuming component of C-SCRM operations and must therefore be designed for efficient execution at scale with dedicated support resources, templated workflows, and automation wherever possible.

4.1.C SCRM Template

4.1.1. Authority & Compliance

List of the laws, executive orders, directives, regulations, policies, standards, and guidelines that govern C-SCRA execution.

Sample Text

- Legislation
  - Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology of 2018
- Policies
  - [Organization Name] C-SCRA Standard Operating Procedures
  - [Organization Name] C-SCRA Risk Assessment Factors
  - [Organization Name] C-SCRA Criticality Assessment Criteria
- Guidelines
  - NIST 800-53 Revision 5: PM-30, RA-3, SA-15, SR-5
  - NIST 800-37 Revision 2
  - NIST 800-161 Revision 1: Appendix C
  - ISO 28001:2007

[41] A supplier may also refer to a source, as defined in the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology of 2018

4.1.2. Description

Describe the purpose and scope of the C-SCRA template, referencing the organizational commitment to C-SCRM and mandate to perform C-SCRAs as an extension of that commitment. Outline the templates relationship to organizational risk management principles, frameworks, practices. This may include providing an overview of the organization's C-SCRA processes, standard operating procedures, and/or criticality designations that govern usage of this template.

Reinforce the business case for executing C-SCRAs by highlighting the benefits of reducing expected loss from adverse cyber supply chain events, as well as the C-SCRM PMOs role in executing these assessments efficiently at scale.

Provide an overview of the organizational boundaries, systems, and services within the scope of the C-SCRAs.

List the contact information and other resources that readers may access in order to further engage with the C-SCRA process.

Sample Text

This C-SCRA is intended to evaluate risks, in a fair and consistent manner, posed to the [Organization] via third parties that hold the potential for harm or compromise arising as a result of cybersecurity risks. Cyber supply chain risks include exposures, threats, and vulnerabilities associated with the products and services traversing the supply chain as well as the exposures, threats, and vulnerabilities to the supply chain and its suppliers.

The C-SCRA template provides tactical guidelines for the [Organization's C-SCRM PMO] to review cyber supply chain risks and ensure that C-SCRAs are appropriately carried out in line with organizational mandates efficiently and effectively.

Requestors seeking to introduce third party products, services, or suppliers into organizational boundaries should familiarize themselves with the following template. This will ensure that requestors can provide the requisite information to the C-SCRM PMO to ensure timely execution of C-SCRAs and are otherwise aligned with adhering to the steps of the C-SCRA.

The C-SCRA process contains five primary steps, as outlined in the below template:[42]

1. Information Gathering & Scoping Analysis
2. Threat Analysis
3. Vulnerability Analysis
4. Impact Analysis
5. Risk Response Analysis

[42] See Appendix D's "Assess" section for the methodological principles and guidance that underpin these steps.

To learn more about the C-SCRA process and/or submit an assessment request to the C-SCRM PMO, please go to [Organizational intranet page] or contact [C-SCRM PMO email].

4.1.3. Information Gathering & Scoping Analysis

Define the purpose and objectives for the requested C-SCRA, outlining the key information required to appropriately define the system, operations, supporting architecture, and boundaries. Provide key questions to requestors to facilitate collection and analysis of this information. The C-SCRM PMO will then use this information as a baseline for subsequent analyses and data requests.

Sample Text

Supply Chain Risk Management Assessment Scoping Questionnaire		
Section 1: Request Overview	Provide Response:	Response Provided by:
Requestor Name		Acquirer
C-SCRA Purpose and Objective		Acquirer
System Description		Acquirer
Architecture Overview		Acquirer
Boundary Definition		Acquirer
Date of Assessment		Acquirer
Assessor Name		Acquirer
Section 2: Product/Service Internal Risk Overview		
What is the suppliers market share for this particular product/service		Acquirer
What % of this supplier's sales of this product/service does your organization consume?		Acquirer
How widely used will the product or service be in your organization?		Acquirer
Is the product/service manufactured in a geographic location that is considered an area of geopolitical risk for your organization based on it's primary area of operation (e.g., in the United States).		Acquirer
Would switching to an alternative supplier for this product or service constitute significant cost or effort for your organization?		Acquirer
Does your organization have an existing relationship with another supplier for this product/service?		Acquirer
How confident is your organization that they will be able to obtain quality		Acquirer

products/services regardless of major supply chain disruptions, both manmade and natural		
Does your organization maintain a reserve of this product/service?		Acquirer
Is the product/service fit for purpose? (i.e., capable of meeting is objectives or service levels)		Acquirer
Does the product/service perform an essential security function? Please describe		Acquirer
Does the product/service have root access to IT networks, OT systems or sensitive platforms?		Acquirer
Can compromise of the product/service lead to system failure or severe degradation?		Acquirer
Is there a known independent reliable mitigation for compromise leading to system failure or severe degradation?		Acquirer
Does the product/service connect to a platform that is provided by your organization to customers?		Acquirer
Does the product/service transmit, generate, maintain, or process high value data?		Acquirer
Does the product/service have access to systems that transmit, generate, maintain or process high value data (e.g., PII, PHI, PCI)		Acquirer
Does the supplier require physical access to the companies facilities as a result of its provision of the product/service?		Acquirer
Based on holistic consideration of the above responses, how critical is this product/service to your organization (e.g., Critical, High, Moderate, Low)		Acquirer
Section 2: Supplier Overview		
Have you identified the supplier's key suppliers?		Supplier
Did you verify the supplier ownership, both foreign and domestic?		Supplier
If the supplier uses distributors, did you investigate them for potential threats?		Supplier
Is the supplier located in the United States?		Supplier
Has the supplier declared where replacement components will be purchased from?		Supplier
Have all of the suppliers', subcontractors', and suppliers' owners and locations been validated?		Supplier

Does the supplier vet suppliers for threat scenarios?		Supplier
Does the supplier have documents which track part numbers to manufacturers?		Supplier
Can the supplier provide a list of who they procure COTS software from?		Supplier
Does the supplier have counterfeit controls in place?		Supplier
Does the supplier safeguard key program information that may be exposed through interactions with suppliers?		Supplier
Does the supplier perform reviews, inspections, and have safeguards to detect/avoid counterfeit equipment, tampered hardware/software (HW/SW), vulnerable HW/SW, and/or operations security leaks leaks?		Supplier
Does the supplier use industry standards baselines (e.g., CIS, NES) when purchasing software?		Supplier
Does the supplier comply with regulatory and legislation mandates?		Supplier
Does the supplier have procedures for secure maintenance and upgrades following deployment?		Supplier
Section 3: Policies & Procedures		
Does the supplier have definitive policies and procedures that help minimize supply chain risk, including subsidiary sourcing needs?		Supplier
Does the supplier define and manage system criticality and capability?		Supplier
Does everyone associated with the procurement (e.g., supplier, C-SCRM PMO) understand the threats and risks in the subject supply chain?		Supplier
Are all engaged personnel US citizens?		Supplier
Does the supplier have "insider threat" controls in place?		Supplier
Does the supplier verify and monitor all personnel that interact with the subject product, system, or service to know if they pose a threat?		Supplier

Does the supplier use, record, and track risk mitigation activities throughout the life cycle of the product, system, or service?		Supplier
Have all of the supplier's personnel signed non-disclosure agreements?		Supplier
Does the supplier allow its personnel or suppliers to access environments remotely (i.e. from an out of boundary)?		Supplier
Section 4: Logistics (if applicable)		
Does the supplier have documented tracking and version controls in place?		Supplier
Does the supplier analyze events (environmental or man-made) that could interrupt their supply chain?		Supplier
Are the supplier's completed parts controlled, so they are never left unattended or exposed to tampering?		Supplier
Are the supplier's completed parts locked up?		Supplier
Does the C-SCRM PMO have a process that ensures integrity when ordering inventory from the supplier?		Supplier
Does the C-SCRM PMO periodically inspect the supplier's inventory for exposure or tampering?		Supplier
Does the C-SCRM PMO have secure material destruction procedures for unused and scrap parts procured from the supplier?		Supplier
Is there a documented chain of custody for the deployment of products and systems?		Supplier
Section 5: Software Design & Development (if applicable)		
Is the C-SCRM PMO familiar with all the suppliers that will work on the design of the product/system?		Supplier and Manufacturer
Does the supplier align its SDLC to a secure software development standard (e.g., Microsoft Security Development Lifecycle)		Supplier and Manufacturer
Does the supplier perform all development onshore?		Supplier and Manufacturer
Do only United States citizens have access to development environments?		Supplier and Manufacturer
Does the supplier provide cybersecurity training to its developers?		Supplier and Manufacturer
Does the supplier use trusted software development tools?		Supplier and Manufacturer

Is the supplier using trusted information assurance controls to safeguard the development environment (e.g., secure network configurations, strict access controls, dynamic/static vulnerability management tools, penetration testing)?		Supplier and Manufacturer
Does the supplier validate open source software prior to use?		Supplier and Manufacturer
Are the supplier's software compilers continuously monitored?		Supplier and Manufacturer
Does the supplier have codified software test and configuration standards?		Supplier and Manufacturer
Section 6: Product/Service Specific Security (if applicable, one questionnaire per product/service)		
Product / Service Name		Manufacturer
Product Type (s) (Hardware, Software, Service)		Manufacturer
Product / Service Description		Manufacturer
Part Number (if applicable)		Manufacturer
Does the manufacturer implement formal organizational roles and governance responsible for the implementation and oversight of Secure Engineering across the development or manufacturing process for product offerings?		Manufacturer
Does the manufacturer have processes for product integrity conform to any of the following standards (e.g., ISO 27036, SAE AS6171, etc.)?		Manufacturer
Is the product Federal Information Processing Standards (FIPS) compliant? If yes, please provide the FIPS level		Manufacturer
Does the manufacturer document and communicate security control requirements for your hardware, software, or solution offering?		Manufacturer
Has the manufacturer received fines or sanctions from any governmental entity or regulatory body in the past year related to the delivery of the product or service? If yes, please describe.		Manufacturer
Has the manufacturer experienced litigation claims over the past year related to the delivery of the product or service? If yes, please describe		Manufacturer

Does the manufacturer provide a bill of materials (BOM) for the products or service, and components which includes all logic-bearing (e.g., readable/writable/programmable) hardware, firmware, and software?		Manufacturer
For hardware components included in the product or service offering, does the supplier only buy from original equipment manufacturers or licensed resellers?		Supplier
Does the manufacturer have a policy or process to ensure that none of your suppliers or third-party components are on any banned list?		Manufacturer
How does the manufacturer prevent malicious and/or counterfeit IP components within their product offering or solution?		Manufacturer
Does the manufacturer manage the integrity of IP for its product or service offering?		Manufacturer
How does the manufacturer assess, prioritize, and remediate reported product or service vulnerabilities?		Manufacturer
How does the manufacturer ensure that product or service vulnerabilities are remediated in a timely period, reducing the window of opportunity for attackers?		Manufacturer
Does the manufacturer maintain and manage a Product Security Incident Reporting and Response program (PSRT)?		Manufacturer
What is the manufacturer's process to ensure customers and external entities (such as government agencies) are notified of an incident when their product or service is impacted?		Manufacturer

4.1.4. Threat Analysis

Define threat analysis as well as the criteria that will be utilized to assess the threat of the product, service, or supplier being assessed. Include a rubric with categorical definitions to encourage transparency behind assessment results.

Sample Text

The C-SCRA threat analysis evaluates and characterizes the level of threat to the integrity, trustworthiness, and authenticity of the product, service, or supplier as described below.

This analysis is based on a threat actor's capability and intent to compromise or exploit the product, service, or supplier being introduced into the cyber supply chain. Following completion of the analysis, one of the following threat levels is assigned:

- **Critical:** Information indicates adversaries are engaged in subversion, exploitation, or sabotage of the product, service, or supplier.
- **High:** Information indicates adversaries have established an overt or clandestine relationship with the product, service, or supplier, with the capability and intent to engage in subversion, exploitation or sabotage of the supply chain; however, there are no known indications of subversion, exploitation, or sabotage.
- **Moderate:** Information indicates adversaries have the capability but NOT the intent to engage in subversion, exploitation or sabotage of the product, service, or supplier. Conversely, they may have the intent but NOT the capability.
- **Low:** Information indicates adversaries have neither the capability nor the intent to engage in subversion, exploitation, or sabotage of the product, service, or supplier.

To appropriately assign the above threat analysis designation, C-SCRM PMOs and requestors should leverage the Information Gathering & Scoping questionnaire to coordinate collection of information related to the product, service, or supplier's operational details, ownership structure, key management personnel, financial information, business ventures, government restrictions, and potential threats. Additional investigations should be performed against the aforementioned topics if red flags are observed during initial data collection.

4.1.5. Vulnerability Analysis

Define vulnerability analysis as well as the criteria that will be utilized to assess the vulnerability of the product, service, or supplier being assessed. Include a rubric with categorical definitions to encourage transparency behind assessment results.

Sample Text

The C-SCRA vulnerability analysis evaluates and then characterizes the vulnerability of the product, service, or supplier throughout its lifecycle and/or engagement. The analysis includes an assessment of the ease of exploitation by a threat actor with moderate capabilities.
This analysis is based on a threat actor's capability and intent to compromise or exploit the product, service, or supplier being introduced into the cyber supply chain. Following completion of the analysis, one of the following threat levels is assigned:

- **Critical:** The product, service, or supplier contains vulnerabilities that are wholly exposed (physically or logically) and are easily exploitable.
- **High:** The product, service, or supplier contains vulnerabilities that are highly exposed and are reasonably exploitable.
- **Moderate:** The product, service, or supplier contains vulnerabilities that are moderately exposed and would be difficult to exploit.
- **Low:** The product, service, or supplier is not exposed and would be unlikely to be exploited.

To appropriately assign the above vulnerability analysis designation, C-SCRM PMOs and requestors should coordinate to collect information related to the product, service, or supplier's operational details, exploitability, service details, attributes of known vulnerabilities, and mitigation techniques.

4.1.6. Impact Analysis

Define impact analysis as well as the criteria that will be utilized to assess the criticality of the product, service, or supplier being assessed. Include a rubric with categorical definitions to encourage transparency behind assessment results.

Sample Text

The C-SCRA impact analysis evaluates and then characterizes the impact of the product, service, or supplier throughout its lifecycle and/or engagement. The analysis includes an end-to-end functional review to identify critical functions and components based on an assessment of the potential harm caused by the probable loss, damage, or compromise of a product, material, or service to an [Organization's] operations or mission.
Following completion of the analysis, one of the following impact levels is assigned:

- **Critical:** The product, service, or supplier's failure to perform as designed would result in a total organizational failure or a significant and/or unacceptable level of degradation of operations that could only be recovered with exceptional time and resources.
- **High:** The product, service, or supplier's failure to perform as designed would result in severe organizational failure or a significant and/or unacceptable level of degradation of operations that could only be recovered with significant time and resources.
- **Moderate:** The product, service, or supplier's failure to perform as designed would result in serious organizational failure that could readily and quickly managed with no long-term consequences.
- **Low:** The product, service, or supplier's failure to perform as designed would result in very little adverse effects on the organization that could readily and quickly managed with no long-term consequences.

To appropriately assign the above impact analysis designation, C-SCRM PMOs and requestors should coordinate to collect information related to [Organization's] critical functions and components, identification of the intended user environment for the product or service, and supplier information.

4.1.7. Risk Response Analysis

Define risk analysis as well as the criteria that will be utilized to assess the scoring of the product or service being assessed. Include a rubric with categorical definitions to encourage transparency behind assessment results.

Sample Text

The C-SCRA risk score reflects a combined judgement based on likelihood and impact analyses. The likelihood analysis is scored via a combination of the aforementioned threat and vulnerability analysis score, as outlined in the figure below.

Likelihood Level					
Threat	**Vulnerability**				
		Low	Moderate	High	Critical
	Very Likely	Moderately Likely	Highly Likely	Very Likely	Very Likely
	Highly Likely	Moderately Likely	Highly Likely	Highly Likely	Very Likely
	Moderately Likely	Unlikely	Moderately Likely	Highly Likely	Highly Likely
	Unlikely	Unlikely	Unlikely	Moderately Likely	Moderately Likely

The C-SCRA risk score is then aggregated based upon that likelihood score and the impact score. If multiple vulnerabilities are identified for a given product or service, each vulnerability shall be assigned a risk level based upon its likelihood and impact.

Overall Risk Score					
Likelihood (threat and vulnerability)	**Impact**				
		Low	Moderate	High	Critical
	Very Likely	Moderate	High	Critical	Critical
	Highly Likely	Moderate	Moderate	High	Critical
	Moderately Likely	Low	Moderate	High	High
	Unlikely	Low	Low	Moderate	High

The aforementioned risk analyses and scoring provide measures by which [Organization] determines whether or not to proceed with procurement of the product, service, or supplier. Decisions to proceed must weighed against the risk appetite and tolerance across the tiers of the organization, as well as the mitigation strategy that may be put in place to manage the risks as a result of procuring the product, service, or supplier.

4.1.8. Roles & Responsibilities

State those responsible for the C-SCRA policies, as well as its key contributors. Include the role and name of each individual or group, as well contact information where necessary (e.g., organizational affiliation, address, email address, and phone number).

Sample Text

- C-SCRM PMO shall:
  - maintaining C-SCRA policies, procedures, and scoring methodologies
  - performing C-SCRA standard operating procedures
  - liaising with requestors seeking to procure a product, service or supplier
  - reporting C-SCRA results to leadership to help inform organizational risk posture

- Each requestor shall:
  - complete C-SCRA request forms and provide all required information
  - address any information follow-up requests from the C-SCRM PMO resource completing the C-SCRA
  - adhering to any stipulations or mitigations mandated by the C-SCRM PMO following approval of a C-SCRA request.

4.1.9. Definitions

List the key definitions described within the policy, providing organizationally-specific context and examples where needed.

Sample Text

- Procurement: Process of obtaining a system, product, or service.

4.1.10. Revision & Maintenance

Define the required frequency for the C-SCRA template. Maintain a table of revisions to enforce version control. C-SCRA templates are living documents that must be updated and communicated to all appropriate individuals (e.g., staff, contractors, and suppliers).

Sample Text

[Organization's] C-SCRA template must be reviewed at a minimum on an annual basis since changes to laws, policies, standards, guidelines, and controls are dynamic and evolving. Additional criteria that may trigger interim revisions include:

- change of policies that impact the C-SCRA template;
- significant C-SCRM events;
- introduction of new technologies;
- discovery of new vulnerabilities;

- operational or environmental changes
- shortcomings in the C-SCRA template;
- change of scope; and
- other organization-specific criteria.

Sample Version Management Table

Version Number	Date	Description of Change/Revision	Section/Pages Affected	Changes made by Name/Title/Organization

APPENDIX E: GLOSSARY

Term	Definition	Source
Acceptable Risk	A level of residual risk to the organization's operations, assets, or individuals that falls within the defined risk appetite and risk tolerance thresholds set by the organization.	
Acquirer	Organization or entity that acquires or procures a product or service.	[ISO/IEC 15288] (adapted)
Acquisition	Includes all stages of the process of acquiring product or services, beginning with the process for determining the need for the product or services and ending with contract completion and closeout.	[NIST SP 800-64 Rev. 2] (adapted)
Agreement	Mutual acknowledgement of terms and conditions under which a working relationship is conducted or goods are transferred between parties. EXAMPLE: contract, memorandum, or agreement	
Authorization	Authorization to operate: The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.	[NIST SP 800-53 Rev. 5]
Authorization Boundary	All components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected	[NIST SP 800-53 Rev. 5]
Authorizing Official (AO)	A senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation.	[NIST SP 800-53 Rev. 5]

Baseline	Hardware, software, databases, and relevant documentation for an information system at a given point in time.	[CNSSI No. 4009]
C-SCRM Control	A safeguard or countermeasures prescribed for the purpose of reducing or eliminating the likelihood and/or impact/consequences of a cyber supply chain risk.	
Cyber Supply Chain Risk	Cyber supply chain risk is the potential for harm or compromise that arises as a result of cybersecurity risks from suppliers, their supply chains, and their products or services. Cyber supply chain risks arise from threats that exploit vulnerabilities or exposures within products and services traversing the supply chain as well as threats exploiting vulnerabilities or exposures within the supply chain itself.	
Cyber Supply Chain Risk Assessment	Cyber Supply Chain Risk Assessment is a systematic examination of cyber supply chain risks, likelihoods of their occurrence, and potential impacts.	
Cyber Supply Chain Risk Management	A systematic process for managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing risk response strategies to the cyber supply chain risks presented by the supplier, the supplied products and services, or the supply chain.	
Defense-in-Breadth	A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle, including system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement.	[NIST SP 800-53 Rev. 5]
Defense-in-Depth	Information security strategy that integrates people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.	[NIST SP 800-53 Rev. 5]
Degradation	A decline in quality or performance; the process by which the decline is brought about.	

Developer	A general term that includes developers or manufacturers of systems, system components, or system services; systems integrators; suppliers; and product resellers. Development of systems, components, or services can occur internally within organizations or through external entities	[NIST SP 800-53 Rev. 5]
Element	Supply chain element: Organizations, entities, or tools employed for the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and/or disposal of systems and system components.	
Enhanced Overlay	An overlay that adds processes, controls, enhancements, and additional implementation guidance specific to the purpose of the overlay.	
Exposure	Extent to which an organization and/or stakeholder is subject to a risk	[ISO Guide 73:2009] (adapted)
External systems Service Provider	A provider of external system services to an organization through a variety of consumer-producer relationships, including joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.	[NIST SP 800-53 Rev. 5]
External System Service	A system service that is provided by an external service provider and for which the organization has no direct control over the implementation of required security and privacy controls or the assessment of control effectiveness.	[NIST SP 800-53 Rev. 5]
Fit for purpose	Fit for purpose is used informally to describe a process, configuration item, IT service, etc., that is capable of meeting its objectives or service levels. Being fit for purpose requires suitable design, implementation, control, and maintenance.	[ITIL Service Strategy] (adapted)
ICT/OT-related service providers	Any organization or individual providing services which may include authorized access to an ICT or OT system	

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; suppliers; product resellers; and third-party partners.	[ISO/IEC 15288] (adapted); adapted from definition of "developer" from [NIST SP 800-53 Rev. 5]
Supply Chain	Supply chain: Linked set of resources and processes between and among multiple levels of organizations, each of which is an acquirer, that begins with the sourcing of products and services and extends through their life cycle.	[ISO 28001] (adapted)
System Integrator	An organization that customizes (e.g., combines, adds, optimizes) components, systems, and corresponding processes. The integrator function can also be performed by acquirer.	[NISTIR 7622] (adapted)
Cyber Supply Chain Compromise	Cyber supply chain incident (also known as compromise) is an occurrence within the supply chain whereby the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits is jeopardized. A cyber supply chain incident can occur anywhere during the life cycle of the system, product or service.	
Information and Communications Technology (ICT)	Encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information.	[ISO/IEC 2382] (adapted)
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.	[NIST SP 800-53 Rev. 5]
Life cycle	Evolution of a system, product, service, project, or other human-made entity.	[ISO/IEC 15288] (adapted)
Likelihood	Chance of something happening	[ISO/IEC 27000:2018]
Organizational Users	An organizational employee or an individual the organization deemed to have similar status of an employee including, for example, contractor, guest researcher, or individual detailed from another organization.	[NIST SP 800-53 Rev. 4] (adapted)

Overlay	A specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.	[NIST SP 800-53 Rev. 5]
Pedigree	The validation of the internal composition and provenance of technologies, products, and services is referred to as the pedigree. For microelectronics, this includes material composition of components. For software this includes the composition of open source and proprietary code, including the version of the component at a given point in time. Pedigrees increase the assurance that the claims suppliers assert about the internal composition and provenance of the products, services, and technologies they provide are valid.	
Provenance	The chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data.	[NIST SP 800-53 Rev. 5]
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.	[NIST SP 800-39]
Residual Risk	Portion of risk remaining after controls/counterrmeasures measures have been applied.	[NIST SP 800-16] (adapted)
Risk Appetite	The types and amount of risk, on a broad level, it is willing to accept in its pursuit of value	[NISTIR 8286]
Risk Framing	The set of assumptions, constraints, risk tolerances, and priorities/trade-offs that shape an organization's approach for managing risk	[NIST SP 800-39]

Risk Management	The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.	[NIST SP 800-53 Rev. 5]
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.	[NIST SP 800-53 Rev. 5]
Risk Response	Intentional and informed decision and actions to accept, avoid, mitigate, share, or transfer an identified risk	[NIST SP 800-53 Rev. 5] (adapted)
Risk Response Plan	A summary of potential consequence(s) of the successful exploitation of a specific vulnerability or vulnerabilities by a threat agent, as well as mitigating strategies and C-SCRM controls	
Risk Tolerance	the organization or stakeholders' readiness to bear the remaining risk after responding to or considering the risk in order to achieve its objectives	[NIST 8286]
Secondary market	An unofficial, unauthorized, or unintended distribution channel.	
Security Control	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.	[NIST SP 800-53 Rev. 5]
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; suppliers; product resellers; and third-party partners.	[ISO/IEC 15288] (adapted)]

System	Combination of interacting elements organized to achieve one or more stated purposes. *Note 1:* There are many types of systems. Examples include: general and special-purpose information systems; command, control, and communication systems; crypto modules; central processing unit and graphics processor boards; industrial control systems; flight control systems; weapons, targeting, and fire control systems; medical devices and treatment systems; financial, banking, and merchandising transaction systems; and social networking systems. *Note 2:* The interacting elements in the definition of system include hardware, software, data, humans, processes, facilities, materials, and naturally occurring physical entities. *Note 3:* System-of-systems is included in the definition of system.	[NIST SP 800-53 Rev. 5] (adapted)
System Component	A discrete identifiable information or operational technology asset that represents a building block of a system and may include hardware, software, and firmware.	
System Development Life Cycle (SDLC)	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal.	[NIST SP 800-34 Rev. 1] (adapted)
System Integrator	Those organizations that provide customized services to the acquirer including for example, custom development, test, operations, and maintenance.	
System Assurance	The justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle.	[NDIA]
System Owner	System owner (or program manager): Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of a system.	[NIST SP 800-53 Rev. 5]

Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	[NIST SP 800-53 Rev. 5]
Threat Assessment/Analysis	Formal description and evaluation of threat to a system or organization.	[NIST SP 800-53 Rev. 5] (adapted)
Threat Event	An event or situation that has the potential for causing undesirable consequences or impact.	[NIST SP 800-30 Rev. 1]
Threat Event Outcome	The effect a threat acting upon a vulnerability has on the confidentiality, integrity, and/or availability of the organization's operations, assets, or individuals.	
Threat Scenario	A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time.	[NIST SP 800-30 Rev. 1]
Threat Source	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.	[NIST SP 800-53 Rev. 5]
Trust	The confidence one element has in another, that the second element will behave as expected.	[Software Assurance in Acquisition: Mitigating Risks to the Enterprise]
Trustworthiness	The interdependent combination of attributes of a person, system, or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities. The degree to which a system (including the technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats.	[NIST SP 800-53 Rev. 5] (adapted)
Validation	confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been	[ISO 9000]

	fulfilled Note: The requirements were met.	
Verification	confirmation, through the provision of objective evidence, that specified requirements have been fulfilled Note: The intended output is correct.	[CNSSI No. 4009], [ISO 9000] (adapted)
Visibility (also Transparency)	Amount of information that can be gathered about a supplier, product, or service and how far through the supply chain this information can be obtained	[ISO/IEC 27036-2] (adapted)
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.	[NIST SP 800-53 Rev. 5]
Vulnerability Assessment	Systematic examination of a system or product or supply chain element to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.	[NIST SP 800-53 Rev. 5] (adapted)

8423
8424
8425

APPENDIX F: ACRONYMS

A&A	Assessment and Authorization
AO	Authorizing Official
API	Application Programming Interface
APT	Advanced Persistent Threat
BIA	Business Impact Analysis
BYOD	Bring Your Own Device
CAC	Common Access Card
CAO	Chief Acquisition Officer
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CLO	Chief Legal Officer
COO	Chief Operating Officer
CPO	Chief Privacy Officer
CRO	Chief Risk Officer
CTO	Chief Technology Officer
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CONUS	Continental United States
COSO	Committee of Sponsoring Organizations of the Treadway Commission'
COTS	Commercial Off-The-Shelf
CRO	Chief Risk Officer

C-SCRM	Cyber Supply Chain Risk Management
CSF	Cybersecurity Framework
CTO	Chief Technology Officer
CUI	Controlled Unclassified Information
CVE	Common Vulnerability Enumeration
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
DMEA	Defense Microelectronics Activity
DoD	Department of Defense
DODI	Department of Defense Instruction
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
FAR	Federal Acquisition Regulation
FARM	Frame, Assess, Respond, Monitor
FASC	Federal Acquisition Security Council
FASCA	Federal Acquisition Supply Chain Security Act
FBI	Federal Bureau of Investigation
FedRAMP	Federal Risk and Authorization Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FITARA	Federal Information Technology Acquisition Reform Act
FOCI	Foreign Ownership, Control or Influence
FSP	Financial Services Cybersecurity Framework Profile
GAO	Government Accountability Office
GIDEP	Government-Industry Data Exchange Program

GOTS	Government Off-The-Shelf
GPS	Global Positioning System
HR	Human Resources
IA	Information Assurance
ICT	Information and Communication Technology
ICT/OT	Information, communications, and operational technology
IDE	Integrated Development Environment
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IOT	Internet of Things
IP	Internet Protocol/Intellectual Property
ISA	Information Sharing Agency
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITL	Information Technology Laboratory (NIST)
JWICS	Joint Worldwide Intelligence Communications System
KPI	Key Performance Indicators
KRI	Key Risk Indicators
KSA	Knowledge, Skills, and Abilities
MECE	Mutually Exclusive and Collectively Exhaustive
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NCCIC	National Cybersecurity and Communications Integration Center

NDI	Non-developmental Items
NDIA	National Defense Industrial Association
NIAP	National Information Assurance Partnership
NICE	National Initiative for Cybersecurity Education
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
OCONUS	Outside of Continental United States
OEM	Original Equipment Manufacturer
OGC	Office of the General Counsel
OMB	Office of Management and Budget
OPSEC	Operations Security
OSS	Open Source Solutions
OSY	Office of Security
OT	Operations Technology
OTS	Off-The-Shelf
OTTF	Open Group Trusted Technology Forum
O-TTPS	Open Trusted Technology Provider™ Standard
OWASP	Open Web Application Security Project
PACS	Physical Access Control System
PII	Personally identifiable information
PIV	Personal Identity Verification
PM	Program Manager
PMO	Program Management Office
POA&M	Plan of Action & Milestones
QA/QC	Quality Assurance/Quality Control
R&D	Research and Development

RFI	Request for Information
RFP	Request for Proposal
RFQ	Request for Questions
RMF	Risk Management Framework
SAFECode	Software Assurance Forum for Excellence in Code
SCIF	Sensitive Compartmented Information Facility
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SECURE	Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (Technology Act)
SLA	Service-Level Agreement
SME	Subject Matter Expert
SOO	Statement of Objective
SOW	Statement of Work
SP	Special Publication (NIST)
SSP	System Security Plan
SWA	Software Assurance
SWID	Software Identification Tag
TTP	Tactics, Techniques, and Procedures
U.S.	United States (of America)
US CERT	United States Computer Emergency Readiness Team

8427

APPENDIX G: REFERENCES

[18 U.S.C.] 18 U.S.C. § 2320.

[41 U.S.C.] 41 U.S.C.

[48 C.F.R.] 48 C.F.R.

[ANSI/NASPO] *ANSI / NASPO Security Assurance Standard*, American National Standards Institute / North American Security Products Organization, 2008.

[ITIL Service Strategy] Cannon, David, *ITIL Service Strategy*, 2nd Edition, The Stationary Office,, July 29, 2011.

[COSO 2011] Thought Leadership in ERM, *Enterprise Risk Management: Understanding and Communicating Risk Appetite,* Committee of Sponsoring Organization of the Treadway Commission (COSO), 2012, https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf.

[COSO 2020] Thought Leadership in ERM, *Risk Appetite – Critical to Success: Using Risk Appetite To Thrive in a Changing World,* Committee of Sponsoring Organization of the Treadway Commission (COSO), 2020, https://www.coso.org/Documents/COSO-Guidance-Risk-Appetite-Critical-to-Success.pdf.

[CISA TEWG] Cybersecurity and Infrasturcture Agency (CISA), *Information and Communications Technology Supply Chain Risk Management Task Force – Threat Evaluation Working Group: Threat Scenarios,*Version 2.0, Arlington, Virginia, 2021, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v2.pdf.

[CISA SCRM WG4] Cybersecurity and Infrastructure Agency (CISA), *Vendor Supply Chain Risk Management (SCRM) Template,* Arlignton, Viriginia, 2021, https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Vendor-SCRM-Template_508.pdf

[Defense Industrial Base Assessment: Counterfeit Electronics] *Defense Industrial Base Assessment: Counterfeit Electronics,* U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, January 2010, https://www.bis.doc.gov/index.php/documents/technology-evaluation/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010/file.

[FEDRAMP] *FedRAMP*, http://www.fedramp.gov/.

[Gardner] Gardner, John T. and Cooper, Martha C., "Strategic Supply Chain Mapping Approaches," *Journal of Business Logistics*, 24 (2003), doi:10.1002/j.2158-1592.2003.tb00045.x.

[GAO] Government Accountability Office (GAO) Report, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks,* U.S. Government Accountability Office, Washington D.C., 2020, https://www.gao.gov/assets/gao-21-171.pdf.

[IRM[Institute of Risk Management, *Risk Appetite & Tolerance Guidance Paper*, London, UK, 2011, https://www.iia.nl/SiteFiles/IRMGuidancePaper-Sep2011.pdf.

[NIAP-CCEVS] *Common Criteria Evaluation & Validation Scheme*, National Information Assurance Partnership, https://www.niap-ccevs.org/.

[NIST SCRM Proceedings 2012] *Summary of the Workshop on Information and Communication Technologies Supply Chain Risk Management*, Gaithersburg, MD, 2012, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=913338.

[SwA] *Software Assurance in Acquisition: Mitigating Risks to the Enterprise. A Reference Guide for Security-Enhanced Software Acquisition and Outsourcing,* DoD & DHS SwA Acquisition Working Group, 2008, https://apps.dtic.mil/dtic/tr/fulltext/u2/a495389.pdf.

[SAFECode 1] Software Assurance Forum for Excellence in Code (Safecode), *Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain*, 2010, http://www.safecode.org/publications/SAFECode_Software_Integrity_Controls0610.pdf.

[SAFECode 2] Software Assurance Forum for Excellence in Code (Safecode), *The Software Supply Chain Integrity Framework: Defining Risks and Responsibilities for Securing Software in the Global Supply Chain*, 2009, http://www.safecode.org/publication/SAFECode_Supply_Chain0709.pdf.

[O-TTPS] The Open Group, Open Trusted Technology Provider™ Standard (O-TTPS), Version 1.1.1, *Mitigating Maliciously Tainted and Counterfeit Products: Part 1: Requirements and Recommendations*, Open Trusted Technology Provider Standard (O-TTPS), 2018, https://publications.opengroup.org/c185-1.

[O-TTPS] The Open Group, Open Trusted Technology Provider™ Standard (O-TTPS), Version 1.1.1, *Mitigating Maliciously Tainted and Counterfeit Products: Part 2: Assessment Procedures for the O-TTPS and ISO/IEC*, Open Trusted Technology Provider Standard (O-TTPS), 2018, https://publications.opengroup.org/c185-2.

[CNSSI 4009] *National Security Systems (CNSS) Glossary*, April 26, 2010, https://www.serdp-estcp.org/content/download/47576/453617/file/CNSSI%204009%20Glossary%202015.pdf.

[DHS SSPD 4300A] *Department of Homeland Security (DHS) Sensitive Systems Policy Directive 4300A,* Department of Homeland Security (DHS), 2011, http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf.

[DODI 5200.39] Department of Defense Instruction (DODI) 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense* U.S. Department of Defense, 2010, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520039p.pdf.

[FAR] *Federal Acquisition Regulation (FAR)*, Acquisition Central, https://acquisition.gov/far/.

[FASCA] Federal Acquisition Supply Chain Security Act of 2018 (FASCA), T*itle II of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology Act of 2018,* 2018, https://www.congress.gov/115/plaws/publ390/PLAW-115publ390.pdf.

[FIPS 199] Federal Information Systems Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, 2004, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[FIPS 200] Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, 2006, http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

[FSP] The Profile Version 1.0, *Financial Services Cybersecurity Framework Profile Version 1.0,* Cyber Risk Institute, 2020, https://cyberriskinstitute.org/the-profile/.

[ISO 9000] ISO 9000:2015, *Quality Management — Fundamentals and vocabulary*, International Organization for Standardization, 2018, https://www.iso.org/standard/45481.html.

[ISO 9001] ISO 9001:2018, *Quality management systems — Requirements,* International Organization for Standardization, 2018, https://www.iso.org/standard/62085.html.

[ISO 28000] ISO 28000:2007, *Specification for Security Management Systems for the Supply Chain*, International Organization for Standardization, 2007, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44641.

[ISO 28001] ISO 28001:2007, *Security management systems for the supply chain -- Best practices for implementing supply chain security, assessments and plans -- Requirements and guidance*, International Organization for Standardization, 2007, http://www.iso.org/iso/catalogue_detail?csnumber=45654.

[ISO/IEC 2382] ISO/IEC 2382-36:2013, *Information Technology -- Vocabulary*, International Organization for Standardization / International Electrotechnical Commission, 2013, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63598.

[ISO/IEC 12207] ISO/IEC 12207: 2017, *Systems and software engineering -- Software life cycle processes*, International Organization for Standardization / International Electrotechnical Commission, 2017, https://www.iso.org/standard/63712.html.

[ISO/IEC 15288] ISO/IEC 15288:2015, *Systems and software engineering -- System life cycle processes*, International Organization for Standardization / International Electrotechnical Commission, 2015, https://www.iso.org/standard/63711.html.

[ISO/IEC 27000] ISO/IEC 27000:2014, *Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary*, International Organization for Standardization / International Electrotechnical Commission, 2014, http://www.iso.org/iso/catalogue_detail?csnumber=41933.

[ISO/IEC 27001] ISO/IEC 27001:2013, *Information technology -- Security techniques -- Information security management systems -- Requirements*, International Organization for Standardization / International Electrotechnical Commission, 2013, http://www.iso.org/iso/catalogue_detail?csnumber=54534.

[ISO/IEC 27002] ISO/IEC 27002:2013, *Information technology -- Security techniques -- Code of practice for information security controls*, International Organization for Standardization / International Electrotechnical Commission, 2013, http://www.iso.org/iso/catalogue_detail?csnumber=54533.

[ISO/IEC 27036] ISO/IEC 27036-2:2014, *Information technology -- Security techniques -- Information security for supplier relationships*, International Organization for Standardization / International Electrotechnical Commission, 2014, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=59680.

[ISO/IEC 20243] ISO/IEC 20243:2018, – *Information Technology — Open Trusted Technology Provider™ Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products,* International Organization for Standardization / International Electrotechnical Commission, 2018, https://www.iso.org/standard/74399.html.

[IRM] Institute of Risk Management, *Risk Appetite & Tolerance Guidance Paper,* London, 2011 https://www.iia.nl/SiteFiles/IRMGuidancePaper-Sep2011.pdf

[NDIA] National Defense Industrial Association (NDIA) System Assurance Committee, *Engineering for System Assurance*, NDIA, Arlington, VA, 2008, https://www.ndia.org/-/media/sites/ndia/meetings-and-events/divisions/systems-engineering/sse-committee/systems-assurance-guidebook.ashx.

[NISPOM] DoD 5220.22-M: *National Industrial Security Program - Operating Manual (NISPOM),* Department of Defense, 2006, https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodm/522022m.pdf.

[NIST CSF] *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1, National Institute of Standards and Technology, Gaithersburg, MD, 2018,

[NISTIR 7622] NIST Interagency Report (IR) 7622: *Notional Supply Chain Risk Management Practices for Federal Information Systems,* National Institute of Standards and Technology, Gaithersburg, MD, 2012, http://dx.doi.org/10.6028/NIST.IR.7622.

[NISTIR 8179] NIST Interagency Report (IR) 8179: *Criticality Analysis Process Model Prioritizing Systems and Component,* National Institute of Standards and Technology, Gaithersburg, MD, 2018, https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8179.pdf.

[NISTIR 8272] NIST Interagency Report (IR) 8272: *Impact Analysis Tool for Interdependent Cyber Supply Chain Risks,* National Institute of Standards and Technology, Gaithersburg, MD, 2020, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8272.pdf.

[NISTIR 8276] NIST Interagency Report (IR) 8276: *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry,* National Institute of Standards and Technology, Gaithersburg, MD, 2021, https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf.

[NISTIR 8286] NIST Interagency Report (IR) 8286: *Integrating Cybersecurity and Enterprise Risk Management (ERM),* National Institute of Standards and Technology, Gaithersburg, MD, 2020, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf.

[NIST SP 800-30 Rev. 1] NIST Special Publication (SP) 800-30 Revision 1, *Guide for Conducting Risk Assessments,* National Institute of Standards and Technology, Gaithersburg, MD, 2012, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

[NIST SP 800-32] NIST Special Publication (SP) 800-32: *Introduction to Public Key Technology and the Federal PKI Infrastructure,* National Institute of Standards and Technology, Gaithersburg, MD, 2001, http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf.

[NIST SP 800-34 Rev. 1] NIST Special Publication (SP) 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems,* National Institute of Standards and Technology, Gaithersburg, MD, 2010, http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.

[NIST SP 800-37] NIST Special Publication (SP) 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* National Institute of Standards and Technology, Gaithersburg, MD, 2018, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[NIST SP 800-39] NIST Special Publication (SP) 800-39, *Managing Information Security Risk,* National Institute of Standards and Technology, Gaithersburg, MD, 2011, http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

[NIST SP 800-53 Rev. 5] NIST Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations,* National Institute of Standards and Technology, Gaithersburg, Maryland, 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[NIST SP 800-53A Rev. 4] NIST Special Publication (SP) 800-53A Revision 4, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans,* National Institute of Standards and Technology, Gaithersburg, MD, 2014, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.

[NIST SP 800-53B Rev. 5] NIST Special Publication (SP) 800-53B Revision 5, *Control Baselines for Information Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf.

[NIST SP 800-100] NIST Special Publication (SP) 800-100, *Information Security Handbook: A Guide for Managers,* National Institute of Standards and Technology, 2006, http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf.

[NIST SP 800-115] NIST Special Publication (SP) 800-115, *Technical Guide to Information Security Testing and Assessment,* National Institute of Standards and Technology, Gaithersburg, MD, 2008, http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

[NIST SP 800-160 Vol. 1] NIST Special Publication (SP) 800-160 Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems,* National Institute of Standards and Technology, Gaithersburg, MD, 2016, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf.

[NIST SP 800-181 Rev. 1] NIST Special Publication (SP) 800-181, *Workforce Framework for Cybersecurity (NICE Framework),* National Institute of Standards and Technology, Gaithersburg, MD, 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.

[OMB A-76] OMB Circular A-76, *Performance of Commercial Activities,* Office of Management and Budget, 2003, https://obamawhitehouse.archives.gov/omb/circulars_a076_a76_incl_tech_correction/.