NIST Special Publication
NIST SP 800-161r1

Cybersecurity 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

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

NIST Special Publication
NIST SP 800-161r1

Cybersecurity 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

May 2022

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

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for 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 800-161r1
Natl. Inst. Stand. Technol. Spec. Publ. 800-161r1, 326 pages (May 2022)
CODEN: NSPUE2

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

Submit comments on this publication to: scrm-nist@nist.gov

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

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 potentially contain malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the 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 or the processes, procedures, standards, and practices used to ensure the security, resilience, reliability, safety, integrity, and quality of the products and services.

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

Keywords

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

Acknowledgments

The authors – Jon Boyens of the 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 Alexander Nelson (NIST), Murugiah Souppaya (NIST), Paul Black (NIST), Victoria Pillitteri (NIST), Kevin Stine (NIST), Stephen Quinn (NIST), Nahla Ivy (NIST), Isabel Van Wyk (NIST), Jim Foti (NIST), Matthew Barrett (Cyber ESI), Greg Witte (Huntington Ingalls), R.K. Gardner (New World Technology Partners), David A. Wheeler (Linux Foundation), Karen Scarfone (Scarfone Cybersecurity), Natalie Lehr-Lopez (ODNI/NCSC), Halley Farrell (BCG), and the original authors of NIST SP 800-161, Celia Paulsen (NIST), Rama Moorthy (Hatha Systems), and Stephanie Shankles (U.S. Department of Veterans Affairs) for their contributions. The authors would also like to thank the C-SCRM community, which has provided invaluable insight and diverse perspectives for managing the supply chain, especially the departments and agencies who shared their experience and documentation on NIST SP 800-161 implementation since its release in 2015, as well as the public and private members of the Enduring Security Framework who collaborated to provide input to Appendix F.

Patent Disclosure Notice

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

List of Figures

List of Tables

1. INTRODUCTION

Information and communications technology (ICT) and operational technology (OT) rely on a complex, globally distributed, extensive, and interconnected supply chain ecosystem that is comprised of 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] that interact to research, develop, design, manufacture, acquire, deliver, integrate, operate, maintain, dispose of, and otherwise utilize or manage ICT/OT products and services. These interactions are shaped and influenced by a set of technologies, laws, policies, procedures, and practices.

This ecosystem has evolved to provide a set of highly refined, cost-effective, and reusable solutions. Public and private sector entities have rapidly adopted this ecosystem of solutions and increased their reliance on commercially available products, system integrator support for custom-built systems, and external service providers. This, in turn, has increased the complexity, diversity, and scale of these entities.

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

Given the definition of supply chain, ***cybersecurity risks throughout the supply chain***[2,3] refers to the potential for harm or compromise that may arise from suppliers, their supply chains, their products, or their services. Cybersecurity risks throughout the supply chain are the results of threats that exploit vulnerabilities or exposures within products and services that traverse the supply chain or threats that exploit vulnerabilities or exposures within the supply chain itself. Examples of cybersecurity risks throughout the supply chain include:

1) A widget manufacturer whose design material is stolen in another country, resulting in the loss of intellectual property and market share.

2) A widget manufacture that experiences a supply disruption for critical manufacturing components due to a ransomware attack at a supplier three tiers down in the supply chain.

3) A store chain that experiences a massive data breach tied to an HVAC vendor with access to the store chain's data-sharing portal.

Note that SCRM and C-SCRM refer to the same concept for the purposes of NIST publications. In general practice, C-SCRM is at the nexus of traditional Supply Chain Risk Management

[1] See the Glossary for definitions for suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.
[2] In the 2015 version of SP 800-161, NIST used the term "ICT supply chain." In this revision, NIST has intentionally moved away from this term as cybersecurity risks can arise in all product and service supply chains, including both ICT and non-technology supply chains.
[3] In an effort to harmonize terminology, the expression "cybersecurity risk in supply chains" should be considered equivalent to "cyber risk in supply chains" for the purposes of this document. In the same manner, the expression "cybersecurity supply chain risk management" should be considered equivalent to "cyber supply chain risk management."

(SCRM) and traditional Information Security. Organizations may employ different terms and definitions for SCRM outside of the scope of this publication. This publication does not address many of the non-cybersecurity aspects of SCRM.

Technology solutions provided through a supply chain of competing vendors offer significant benefits, including low cost, interoperability, rapid innovation, and product feature variety. Whether proprietary, government-developed, or open source, these solutions can meet the needs of a global base of public and private sector customers. However, the same factors that create such benefits also increase the potential for cybersecurity risks that arise directly or indirectly from the supply chain. Cybersecurity risks throughout the supply chain are often undetected and impact the acquirer and the end-user. For example, deployed software is typically a commercial off-the-shelf (COTS) product, which includes smaller COTS or open source software components developed or sourced at multiple tiers. Updates to software deployed across enterprises often fail to update the smaller COTS components with known vulnerabilities, including cases in which the component vulnerabilities are exploitable in the larger enterprise software. Software users may be unable to detect the smaller known vulnerable components in larger COTS software (e.g., lack of transparency, insufficient vulnerability management, etc.). The non-standardized nature of C-SCRM practices adds an additional layer of complexity as this makes the consistent measurement and management of cybersecurity risks throughout the supply chain difficult for both the organization and members of its supply chain (e.g., suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers).

In this document, the practices and controls described for Cybersecurity Supply Chain Risk Management (C-SCRM) apply to both information technology (IT) and operational technology (OT) environments and is inclusive of IoT. Similar to IT environments that rely on ICT products and services, OT environments rely on OT and ICT products and services, with cybersecurity risks arising from ICT/OT products, services, suppliers, and their supply chains. Enterprises 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 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 reports on the progress and effectiveness of the agency's supply chain risk management, consistent with guidance issued by the Office of Management and Budget (OMB) and the Council.

Note that this publication uses the term "enterprise" to describe Level 1 of the risk management hierarchy. In practice, an organization is defined as an entity of any size, complexity, or positioning within a larger enterprise structure (e.g., a federal agency or company). By this definition, an enterprise is an organization, but it exists at the top level of the hierarchy where individual senior leaders have unique risk management responsibilities [NISTIR 8286]. Several organizations may comprise an enterprise. In these cases, an enterprise may have multiple Level 1s with stakeholders and activities defined at both the enterprise and the organization levels. Level 1 activities conducted at the enterprise level should inform those activities completed within the subordinate organizations. Enterprises and organizations tailor the C-SCRM practices described in this publication as applicable and appropriate based on their own unique enterprise structure. There are cases in this publication in which the term "organization" is inherited from a referenced source (e.g., other NIST publication, regulatory language). Refer to NISTIR 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*, for further guidance on this topic.

1.1. Purpose

Cybersecurity Supply Chain Risk Management (C-SCRM) is a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures. The purpose of this publication is to provide guidance to enterprises on how to identify, assess, select, and implement risk management processes and mitigating controls across the enterprise to help manage cybersecurity risks throughout the supply chain. The content in this guidance is the shared responsibility of different disciplines with different SCRM perspectives, authorities, and legal considerations.

The C-SCRM guidance provided in this document is not one-size-fits-all. Instead, the guidance throughout this publication should be adopted and tailored to the unique size, resources, and risk circumstances of each enterprise. Enterprises adopting this guidance may vary in how they implement C-SCRM practices internally. To that end, this publication describes C-SCRM practices observed in enterprises and offers a general prioritization of C-SCRM practices (i.e., Foundational, Sustaining, Enabling)[4] for enterprises to consider as they implement and mature C-SCRM. However, this publication does not offer a specific roadmap for enterprises to follow to reach various states of capability and maturity.

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

1.2. Target Audience

C-SCRM is an enterprise-wide activity that should be directed as such from a governance perspective, regardless of the specific enterprise 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, chief 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 project management-related responsibilities, including certified project managers and/or integrated project team (IPT) members;
- Individuals with acquisition and procurement-related responsibilities, including acquisition officials and contracting officers;

[4] Refer to Section 3.4 of this publication.

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

1.3. Guidance for Cloud Service Providers

The *external system service providers* discussed in this publication include *cloud service providers*. This publication does not replace the guidance provided with respect to federal agency assessments 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 this document for those processes and controls that are not addressed by FedRAMP.[5]

1.4. Audience Profiles and Document Use Guidance

Given the wide audience of this publication, several reader profiles have been defined to point readers to the sections of the document that most closely pertain to their use case. Some readers will belong to multiple profiles and should consider reading all applicable sections. Any reader accountable for the implementation of a C-SCRM capability or function within their enterprise, regardless of role, should consider the entire document applicable to their use case.

1.4.1. Enterprise Risk Management and C-SCRM Owners and Operators

These readers are those responsible for enterprise risk management and cybersecurity supply chain risk management. These readers may help develop C-SCRM policies and standards, perform assessments of cybersecurity risks throughout the supply chain, and serve as subject matter experts for the rest of the enterprise. The entire document is relevant to and recommended for readers fitting this profile.

1.4.2. Enterprise, Agency, and Mission and Business Process Owners and Operators

These readers are the personnel responsible for the activities that create and/or manage risk within the enterprise. They may also own the risk as part of their duties within the mission or business process. They may have responsibilities for managing cybersecurity risks throughout

[5] For cloud services, FedRAMP is applicable for low-, moderate-, high-impact systems [FedRAMP].

the supply chain for the enterprise. Readers in this group may seek general knowledge and guidance on Cybersecurity Supply Chain Risk Management. Recommended reading includes:

- Section 1: Introduction
- Section 2: Integration of C-SCRM into Enterprise-wide Risk Management
- Section 3.3: C-SCRM Awareness and Training
- Section 3.4: C-SCRM Key Practices
- Section 3.6: Dedicated Resources
- Appendix A: C-SCRM Security Controls
- Appendix B: C-SCRM Control Summary
- Appendix E: FASCSA

1.4.3. Acquisition and Procurement Owners and Operators

These readers are those with C-SCRM responsibilities as part of their role in the procurement or acquisition function of an enterprise. Acquisition personnel may execute C-SCRM activities as a part of their general responsibilities in the acquisition and procurement life cycle. These personnel will collaborate closely with the enterprise's C-SCRM personnel to execute C-SCRM activities with acquisition and procurement. Recommended reading includes:

- Section 1: Introduction
- Section 2.1: The Business Case for C-SCRM
- Section 2.2: Cybersecurity Risks Throughout the Supply Chain
- Section 3.1: C-SCRM in Acquisition
- Section 3.3: C-SCRM Awareness and Training
- Appendix A: C-SCRM Security Controls
    - These readers should pay special attention to requisite controls for supplier contracts and include them in agreements with both primary and sub-tier contractor parties.
- Appendix F: Software Supply Chain Security Guidelines

1.4.4. Information Security, Privacy, or Cybersecurity Operators

These readers are those with operational responsibility for protecting the confidentiality, integrity, and availability of the enterprise's critical processes and information systems. As part of those responsibilities, these readers may find themselves directly or indirectly involved with conducting Cybersecurity Supply Chain Risk Assessments and/or the selection and implementation of C-SCRM controls. In smaller enterprises, these personnel may bear the responsibility for implementing C-SCRM and should refer to Section 1.3.1 for guidance. Recommended reading includes:

- Section 1: Introduction
- Section 2.1: The Business Case for C-SCRM
- Section 2.2: Cybersecurity Risks Throughout the Supply Chain
- Section 3.2: Supply Chain Information Sharing

- Section 3.4: C-SCRM Key Practices
- Appendix A: C-SCRM Security Controls
- Appendix B: C-SCRM Control Summary
- Appendix C: Risk Exposure Framework
- Appendix G: C-SCRM Activities in the Risk Management Process
- Appendix E: FASCSA
- Appendix F: Software Supply Chain Security Guidelines

1.4.5. System Development, System Engineering, and System Implementation Personnel

These readers are those with responsibilities for executing activities within an information system's system development life cycle (SDLC). As part of their SDLC responsibilities, these readers will be responsible for the execution of operational-level C-SCRM activities. Specifically, these personnel may be concerned with implementing C-SCRM controls to manage cybersecurity risks that arise from products and services provided through the supply chain within the scope of their information system(s). Recommended reading includes:

- Section 1: Introduction
- Section 2.1: The Business Case for C-SCRM
- Section 2.2: Cybersecurity Risks Throughout the Supply Chain
- Section 2.3.4: Level 3 - Operational
- Appendix A: C-SCRM Security Controls
- Appendix B: C-SCRM Control Summary
- Appendix C: Risk Exposure Framework
- Appendix F: Software Supply Chain Security Guidelines
- Appendix G: C-SCRM Activities in the Risk Management Process

1.5. Background

C-SCRM encompasses activities that span the entire SDLC, including research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, disposal, and the overall management of an enterprise's products and services. Enterprises should integrate C-SCRM within the SDLC as this is a critical area for addressing cybersecurity risks throughout the supply chain. C-SCRM is the organized and purposeful management of cybersecurity risks throughout the supply chain. C-SCRM requires enterprise recognition and awareness, and it lies at the intersections of security, suitability, safety, reliability, usability, quality, integrity, efficiency, maintainability, scalability, and resilience, as depicted in Figure 1-1. These dimensions are layers of consideration for enterprises as they approach C-SCRM and should be positively impacted by C-SCRM.

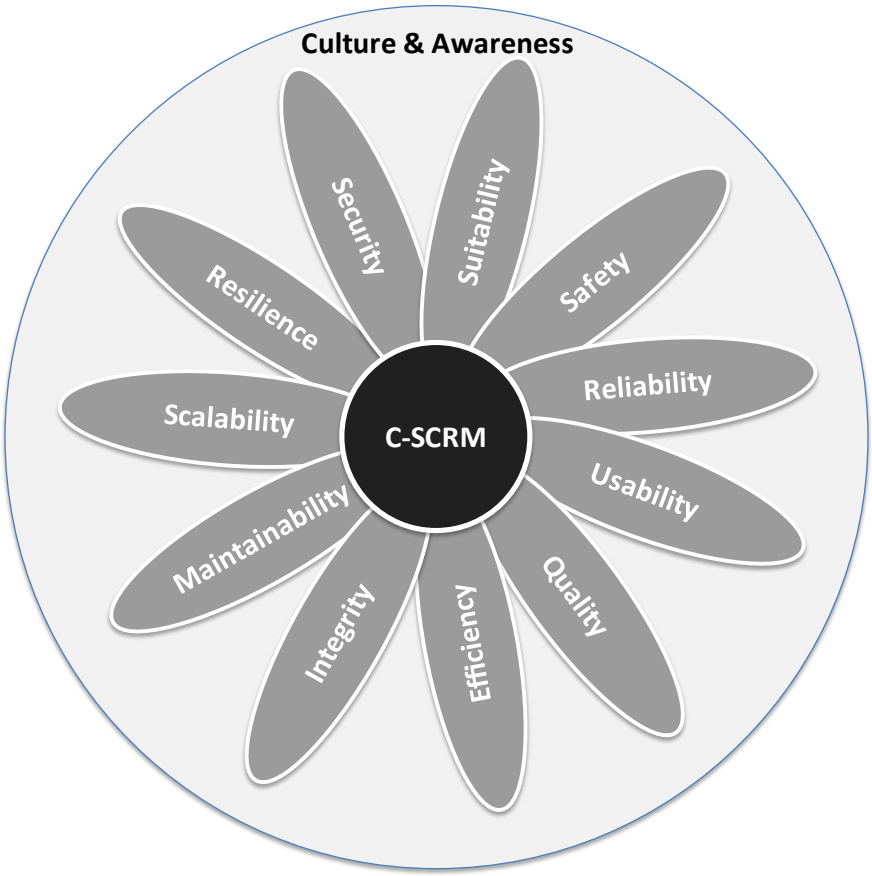

Fig. 1-1: Dimensions of C-SCRM

- **Culture and Awareness** is the set of shared values, practices, goals, and attitudes of the organization that set the stage for successful C-SCRM. It includes a learning process that influences individual and enterprise attitudes and understanding to realize the importance of C-SCRM and the adverse consequences of its failure.[6]
- **Security** provides the confidentiality, integrity, and availability of (a) information that describes the supply chain (e.g., information about the paths of products and services, both logical and physical); (b) information, products, and services that traverse the supply chain (e.g., intellectual property contained in products and services); and/or (c) information about the parties participating in the supply chain (anyone who touches a product or service throughout its life cycle).
- **Suitability** is focused on the supply chain and the provided products and services being right and appropriate for the enterprise and its purpose.
- **Safety** is focused on ensuring that the product or service is free from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. [7]
- **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.[8]

[6] NIST SP 800-16
[7] NIST SP 800-160 Vol.2
[8] NIST SP 800-160 Vol.2

- **Usability** is focused on the extent to which a product or service can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use.[9]
- **Quality** is focused on meeting or exceeding performance, technical, and functional specifications while mitigating vulnerabilities and weaknesses 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.
- **Efficiency** is focused on the timeliness of the intended result delivered by a product or service.
- **Maintainability** is focused on the ease of a product or service to accommodate change and improvements based on past experience in support of expanding future derived benefits.
- **Integrity** is focused on guarding products and the components of products against improper modification or tampering and ensuring authenticity and pedigree.
- **Scalability** is the capacity of a product or service to handle increased growth and demand.
- **Resilience** is focused on ensuring that a product, service, or the supply chain supports the enterprise's ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

1.5.1. Enterprise's Supply Chain

Contemporary enterprises run complex information systems and networks to support their missions. These information systems and networks are composed of ICT/OT[10] products and components made available by *suppliers*, *developers*, and *system integrators*. Enterprises also acquire and deploy an array of products and services, including:

- Custom software for information systems built to be deployed within the enterprise, made available by *developers;*
- Operations, maintenance, and disposal support for information systems and networks within and outside of the enterprise's boundaries,[11] made available by *system integrators or other ICT/OT-related service providers*; and
- External services to support the enterprise's operations that are positioned both inside and outside of the authorization boundaries, made available by *external system service providers*.

[9] NIST SP 800-63-3

[10] 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.

[11] 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.

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

- Performed by the staff employed by the enterprise, developer, system integrator, or external system service provider;
- Physically hosted by the enterprise, 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;
- Proprietary, open source, or commercial off-the-shelf (COTS) hardware and software.

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

1.5.2. Supplier Relationships Within Enterprises

Enterprises depend on the supply chain to provide a variety of products and services to enable the enterprise to achieve its strategic and operational objectives. Identifying cybersecurity risks throughout the supply chain is complicated by the information asymmetry that exists between acquiring enterprises and their suppliers and service providers. Acquirers often lack visibility and understanding of how acquired technology is developed, integrated, and deployed and how the services that they acquire are delivered. Additionally, acquirers with inadequate or absent C-SCRM processes, procedures, and practices may experience increased exposure cybersecurity risks throughout the supply chain. The level of exposure to cybersecurity risks throughout the supply chain depends largely on the relationship between the products and services provided and the criticality of the missions, business processes, and systems that they support. Enterprises have a variety of relationships with their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Figure 1-2 depicts how these diverse relationships affect an enterprise's visibility and control of the supply chain.

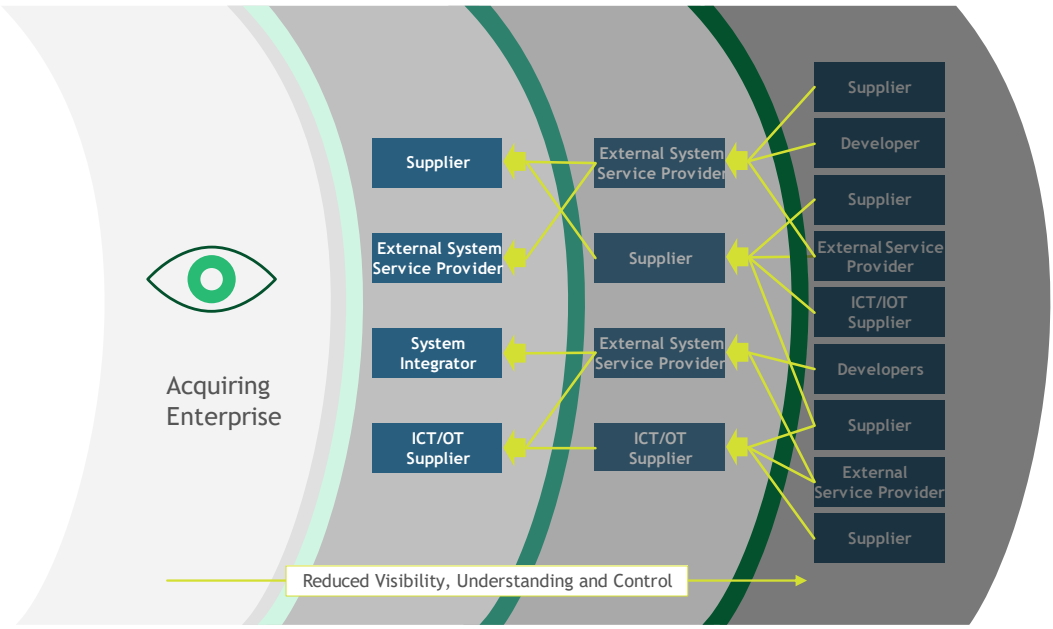

Fig. 1-2: An Enterprise's Visibility, Understanding, and Control of its Supply Chain

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

Procuring ICT/OT products 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 tailored to an individual customer's specific operational or threat environments. Enterprises should perform due diligence and research regarding their specific C-SCRM requirements to determine if an IT solution is fit

for purpose,[12] includes requisite security features and capabilities, will meet quality and resiliency expectations, and requires support by the supplier 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 direct dialogue 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 to make risk-based decisions about product purchases, configurations, and usages within their environment.

Managing Cost and Resources

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

Enterprises should be aware that implementing C-SCRM practices and 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 applications and not tailored to the specific enterprise security or C-SCRM requirements. When deciding whether to require and implement C-SCRM practices and controls, acquirers should consider both the costs of implementing these controls and the risks of not implementing them.

When possible and appropriate, acquirers should allow suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers the opportunity to reuse applicable existing data and documentation that may provide evidence to support C-SCRM (e.g., certification of a vendor to a relevant standard, such as ISO 27001). Doing this results in cost savings to the acquirer and supplier. However, in some cases, documentation reuse may not be appropriate as additional or different information may be needed, and a reassessment may be required (e.g., previously audited supplier developing a new, not yet produced product). Regardless, acquirers should identify and include security considerations early in the acquisition process.

[12] "Fit for purpose" is a term used to informally 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].)

1.6. Methodology for Building C-SCRM Guidance Using NIST SP 800-39; NIST SP 800-37, Rev 2; and NIST SP 800-53, Rev 5

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

The guidance/controls contained in this publication are built on existing multidisciplinary practices and are intended to increase the ability of enterprises to manage the associated cybersecurity risks throughout the supply chain over the entire life cycle of systems, products, and services. It should be noted that this publication gives enterprises 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, this document describes the development and implementation of C-SCRM Strategies and Implementation Plans for development at the enterprise and mission and business level of an enterprise and a C-SCRM system plan at the operational level of an enterprise. A C-SCRM plan at the operational level is informed by the cybersecurity supply chain risk assessments and should contain C-SCRM controls tailored to specific agency mission and business needs, operational environments, and/or implementing technologies.

Integration into the Risk Management Process

The processes in this publication should be integrated into the enterprise's existing SDLCs and enterprise environments at all levels of risk management processes and hierarchy (e.g., enterprise, 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].

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 [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 and RMF-type processes, where possible and applicable. Section 2 and Appendix C describe the linkages between C-SCRM and [NIST SP 800-37, Rev. 2] in further detail.

1.7. Relationship to Other Publications and Publication Summary

This publication builds on the concepts promoted within other NIST publications and tailors those concepts for use within Cybersecurity Supply Chain Risk Management. As a result of this relationship, this publication inherits many of its concepts and looks to other NIST publications to continue advancing base frameworks, concepts, and methodologies. Those NIST publications include:

- **NIST Cybersecurity Framework (CSF) Version 1.1:** Voluntary guidance based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. It was also designed to foster risk and cybersecurity management communications among both internal and external organizational stakeholders.
- **FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*:** A standard for categorizing federal information and information systems according to an agency's level of concern for confidentiality, integrity, and availability and the potential impact on agency assets and operations should their information and information systems be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction.
- **SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*:** Guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in SP 800-39. Risk assessments carried out at all three tiers in the risk management hierarchy are part of an overall risk management process that provides senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks.
- **SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*:** Describes the Risk Management Framework (RMF) and provides guidelines for applying the RMF to information systems and organizations. The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.
- **SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*:** Provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems.
- **SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*:** Provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks.
- **SP 800-53B, *Control Baselines for Information Systems and Organizations*:** Provides security and privacy control baselines for the Federal Government. There are three

security control baselines – one for each system impact level (i.e., low-impact, moderate-impact, and high-impact) – and a privacy baseline that is applied to systems irrespective of impact level;

- **SP 800-160 Vol. 1, *Systems Security Engineering*:** Addresses the engineering-driven perspective and actions necessary to develop more defensible and survivable systems, inclusive of the machine, physical, and human components comprising the systems, capabilities, and services delivered by those systems.
- **SP 800-160 Vol. 2, Revision 1, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*:** A handbook for achieving identified cyber resiliency outcomes based on a systems engineering perspective on system life cycle processes in conjunction with risk management processes, allowing the experience and expertise of the organization to help determine what is correct for its purpose.
- **SP 800-181, Revision 1, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*:** A fundamental reference for describing and sharing information about cybersecurity work. It expresses that work as Task statements and describes Knowledge and Skill statements that provide a foundation for learners, including students, job seekers, and employees.
- **NISTIR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*:** Provides a wide array of practices that help mitigate supply chain risk to federal information systems. It seeks to equip federal departments and agencies with a notional set of repeatable and commercially reasonable supply chain assurance methods and practices that offer a means to obtain an understanding of and visibility throughout the supply chain.
- **NISTIR 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components*:** Helps organizations identify those systems and components that are most vital and which may need additional security or other protections.
- **NISTIR 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*:** Provides a set of Key Practices that any organization can use to manage the cybersecurity risks associated with their supply chains. The Key Practices presented in this document can be used to implement a robust C-SCRM function at an organization of any size, scope, and complexity. These practices combine the information contained in existing C-SCRM government and industry resources with the information gathered during the 2015 and 2019 NIST research initiatives.
- **NISTIR 8286, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)*:** Helps individual organizations within an enterprise improve their cybersecurity risk information, which they provide as inputs to their enterprise's ERM processes through communication and risk information sharing.
- **NISTIR 8286A, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*:** Offers examples and information to illustrate risk tolerance, risk appetite, and methods for determining risks in that context. To support the development of an Enterprise Risk Register, this report describes the documentation of various scenarios based on the potential impact of threats and vulnerabilities on enterprise assets. Documenting the likelihood and impact of various threat events through cybersecurity risk registers integrated into an enterprise risk profile helps to later prioritize and communicate enterprise cybersecurity risk response and monitoring.
- **NISTIR 8286B, *Prioritizing Cybersecurity Risk for Enterprise Risk Management*:** Provides detail regarding stakeholder risk guidance and risk identification and analysis.

This second publication describes the need for determining the priorities of each of those risks in light of their potential impact on enterprise objectives, as well as options for properly treating that risk. This report describes how risk priorities and risk response information are added to the cybersecurity risk register (CSRR) in support of an overall enterprise risk register. Information about the selection of and projected cost of risk response will be used to maintain a composite view of cybersecurity risks throughout the enterprise, which may be used to confirm and adjust risk strategy to ensure mission success.

This publication also draws upon concepts and work from other regulations, government reports, standards, guidelines, and best practices. A full list of those resources can be found in Appendix H.

Key Takeaways[13]

The Supply Chain. ICT/OT relies on a globally distributed, interconnected supply chain ecosystem that consists of public and private sector entities (e.g., acquirers, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers).

Supply Chain Products and Services. Products and services that enterprises rely on the supply chain for include the provision of systems and system components, open source and custom software, operational support services, hosting systems and services, and performing system support roles.

Supply Chain Benefits and Risk. This ecosystem offers benefits such as cost savings, interoperability, rapid innovation, product feature variety, and the ability to choose between competing vendors. However, the same mechanisms that provide those benefits might also introduce a variety of cybersecurity risks throughout the supply chain (e.g., a supplier disruption that causes a reduction in service levels and leads to dissatisfaction from the enterprise's customer base).

Cybersecurity Supply Chain Risk Management (C-SCRM). C-SCRM, as described in this document, is a systematic process that aims to help enterprises manage cybersecurity risks throughout the supply chain. Enterprises should identify, adopt, and tailor the practices described in this document to best suit their unique strategic, operational, and risk context.

Scope of C-SCRM. C-SCRM encompasses a wide array of stakeholder groups that include information security and privacy, system developers and implementers, acquisition, procurement, legal, and HR. C-SCRM covers activities that span the entire system development life cycle (SDLC), from initiation to disposal. In addition, identified cybersecurity risks throughout the supply chain should be aggregated and contextualized as part of enterprise risk management processes to ensure that the enterprise understands the total risk exposure of its critical operations to different risk types (e.g., financial risk, strategic risk).

[13] Key takeaways describe key points from the section text. Refer to the Glossary in Appendix H for definitions.

2. INTEGRATION OF C-SCRM INTO ENTERPRISE-WIDE RISK MANAGEMENT[14]

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:

- *Frame risk*. Establish the context for risk-based decisions and the current state of the enterprise's information and communications technology and services and the associated supply chain.
- *Assess risk*. Review and interpret criticality, threat, vulnerability, likelihood,[15] impact, and related information.
- *Respond to risk*. Select, tailor, and implement mitigation controls based on risk assessment findings.
- *Monitor risk*. Monitor risk exposure and the effectiveness of mitigating risk on an ongoing basis, including tracking changes to an information system or supply chain using effective enterprise communications and a feedback loop for continuous improvement.

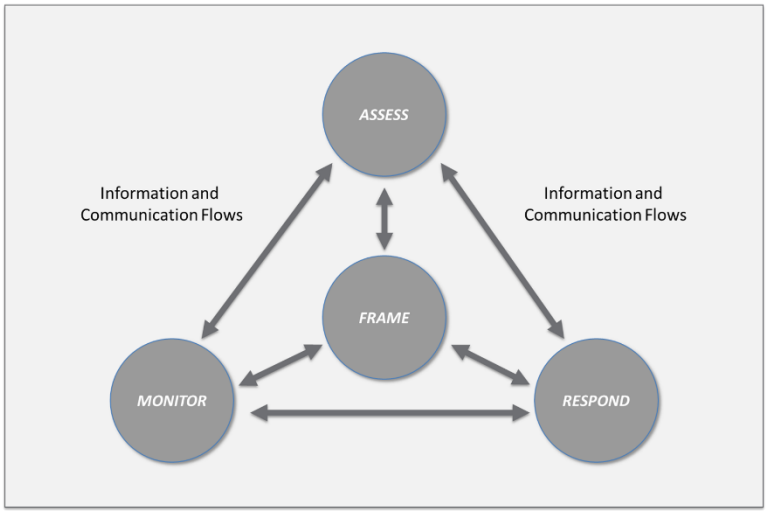

Fig. 2-1: Risk Management Process

Managing cybersecurity risks throughout the supply chain is a complex undertaking that requires cultural transformation and a coordinated, multidisciplinary approach across an enterprise. Effective cybersecurity supply chain risk management (C-SCRM) requires engagement from stakeholders inside the enterprise (e.g., departments, processes) and outside of the enterprise (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. Successful C-SCRM requires an enterprise-wide cultural

[14] Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.
[15] For C-SCRM purposes, likelihood is defined as the probability of a threat exploiting a vulnerability within a given timeframe. It should be noted that in mathematics, likelihood and probability are fundamentally different concepts, but the difference between the two is outside of the scope of this publication.

shift to a state of heightened awareness and preparedness as to the potential ramifications of cybersecurity risks throughout the supply chain.

Enterprises 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 cybersecurity risks throughout the supply chain. Enterprises may define explicit roles to bridge and integrate these processes as a part of an enterprise's broader risk management activities. This orchestrated approach is an integral part of an enterprise's effort to identify C-SCRM priorities, develop solutions, and incorporate C-SCRM into overall risk management decisions. Enterprises should perform C-SCRM activities as a part of the acquisition, SDLC, and broader enterprise risk management processes. Embedded C-SCRM activities involve determining the criticality of functions and their dependency on the supplied products and services, 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 (and sometimes within) enterprises, business and mission-specific strategies, and policies should set the tone and direction for C-SCRM across the enterprise.

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

- Manage rather than eliminate risk as risk is integral to the pursuit of value;
- 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.

2.1. The Business Case for C-SCRM

Today, every enterprise 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 enterprise needs to have to address cybersecurity risks throughout the supply chain that arise from the use of digital technology. The depth, extent, and maturity of a C-SCRM capability for each enterprise should be based on the uniqueness of its business or mission, enterprise-specific compliance requirements, operational environment, risk appetite, and risk tolerance.

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

- An established C-SCRM program will enable enterprises to understand which critical assets are most susceptible to supply chain weaknesses and vulnerabilities.
- C-SCRM reduces the likelihood of supply chain compromise by a cybersecurity threat by enhancing an enterprise's ability to effectively detect, respond, and recover from events that result in significant business disruptions should a C-SCRM compromise occur.

- Operational and enterprise efficiencies are achieved through clear structure, purpose, and alignment with C-SCRM capabilities and the prioritization, consolidation, and streamlining of existing C-SCRM processes.
- There is greater assurance that acquired products are of high quality, authentic, reliable, resilient, maintainable, secure, and safe.
- There is greater assurance that suppliers, service providers, and the technology products and services that they provide are trustworthy and can be relied upon to meet performance requirements.

C-SCRM is fundamental to any effort to manage risk exposure arising from enterprise operations. Implementing C-SCRM processes and controls requires human, tooling, and infrastructure investments by acquirers and their developers, system integrators, external system service providers, and other ICT/OT-related service providers. However, enterprises have finite resources to commit to establishing and deploying C-SCRM processes and controls. As such, enterprises should carefully weigh the potential costs and benefits when making C-SCRM resource commitment decisions and make decisions based on a clear understanding of any risk exposure implications that could arise from a failure to commit the necessary resources to C-SCRM.

While there are cost-benefit trade-offs that must be acknowledged, the need to better secure supply chains is an imperative for both government and the private sector. The passage of the 2018 SECURE Technology Act,[16] the formation of the FASC, and the observations from the 2015 and 2019 Case Studies in Cyber Supply Chain Risk Management captured in NIST Interagency or Internal Report (NISTIR) 8276, *Key Practices in Cyber Supply Chain Risk Management*, point to a broad public and private sector consensus: C-SCRM capabilities are a critical and foundational component of any enterprise's risk posture.

2.2. Cybersecurity Risks Throughout Supply Chains

Cybersecurity risks throughout the supply chain refers to the potential for harm or compromise that arises from the cybersecurity risks posed by suppliers, their supply chains, and their products or services. Examples of these risks include:

- Insiders working on behalf of a system integrator steal sensitive intellectual property, resulting in the loss of a major competitive advantage.[17]
- A proxy working on behalf of a nation-state inserts malicious software into supplier-provided product components used in systems sold to government agencies. A breach occurs and results in the loss of several government contracts.
- A system integrator working on behalf of an agency reuses vulnerable code, leading to a breach of mission-critical data with national security implications.
- An organized criminal enterprise introduces counterfeit products onto the market, resulting in a loss of customer trust and confidence.
- A company is on contract to produce a critical component of a larger acquisition, but the company relabels products from an unvetted supplier. A critical component that cannot

[16] SECURE Technology Act - Public Law 115-390: https://www.govinfo.gov/app/details/COMPS-15413
[17] To qualify as a cybersecurity risk throughout the supply chain, insider threats specifically deal with instances of third-party insider threats.

be trusted is deployed into operational systems, and there no trusted supplier of replacement parts.

Risks such as these are realized when threats in the cybersecurity supply chain exploit existing vulnerabilities. Figure 2-2 depicts supply chain cybersecurity risks resulting from the likelihood that relevant threats may exploit applicable vulnerabilities and the consequential potential impacts.

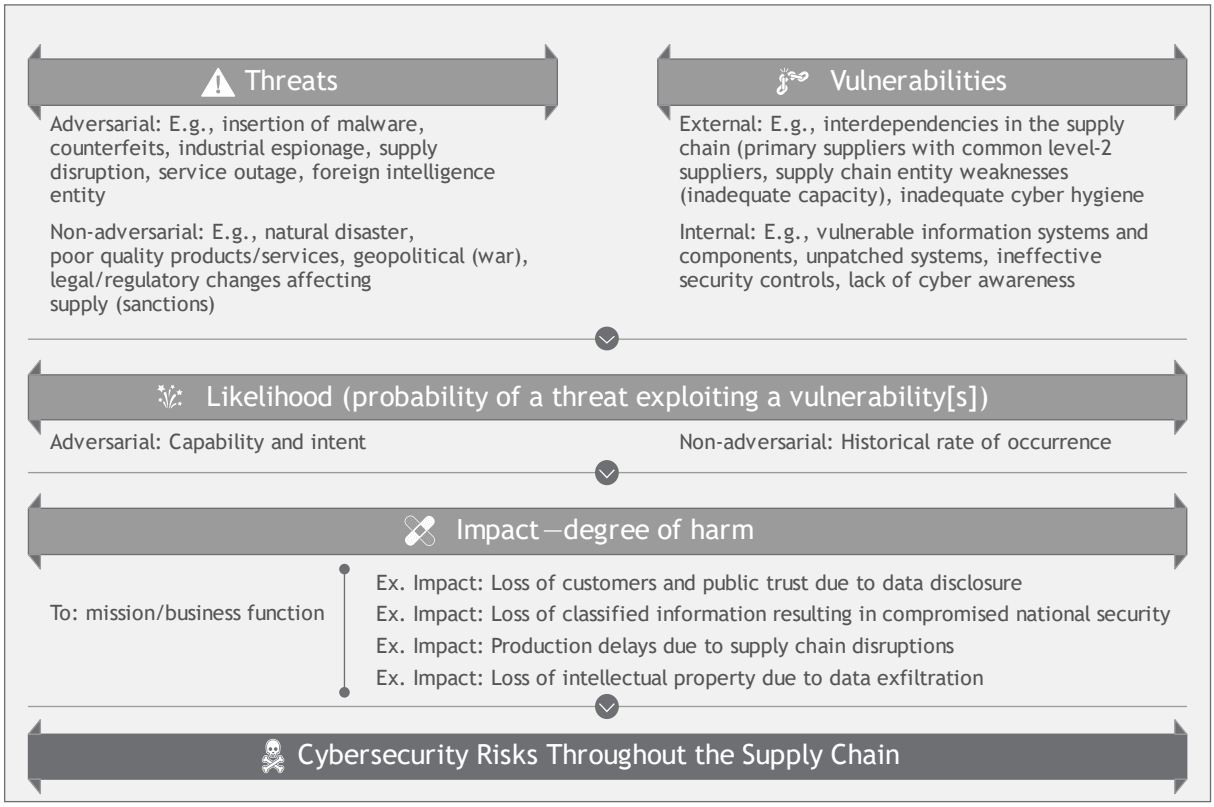

Fig. 2-2: Cybersecurity Risks Throughout the Supply Chain

Supply chain cybersecurity vulnerabilities may lead to persistent negative impacts on an enterprise's missions, ranging from a reduction in service levels leading to customer dissatisfaction to the theft of intellectual property or the degradation of critical mission and business processes. It may, however, take years for such vulnerabilities to be exploited or discovered. It may also be difficult to determine whether an event was the direct result of a supply chain vulnerability. Vulnerabilities in the supply chain are often interconnected and may expose enterprises to cascading cybersecurity risks. For example, a large-scale service outage at a major cloud services provider may cause service or production disruptions for multiple entities within an enterprise's supply chain and lead to negative effects within multiple mission and business processes.

2.3. Multilevel Risk Management[18]

To integrate risk management throughout an enterprise, [NIST SP 800-39] describes three levels, depicted in Figure 2-3, that address risk from different perspectives: 1) the enterprise-level, 2) the mission and business process level, and 3) the operational level. C-SCRM requires the involvement of all three levels.

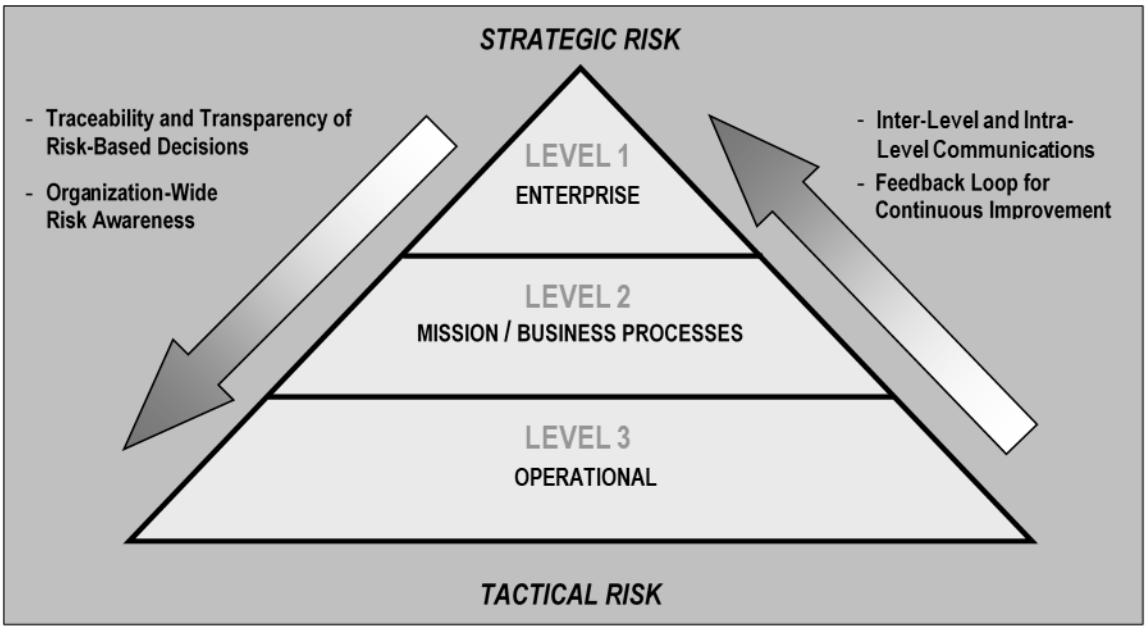

Fig. 2-3: Multilevel Enterprise-Wide Risk Management[19]

In multilevel risk management, the C-SCRM process is seamlessly carried out across the three tiers with the overall objective of continuous improvement in the enterprise's risk-related activities and effective inter- and intra-level communication among stakeholders with a vested interest in C-SCRM.

C-SCRM activities can be performed by a variety of individuals or groups within an enterprise, ranging from a single individual to committees, divisions, centralized program offices, or any other enterprise structure. C-SCRM activities are distinct for different enterprises depending on their structure, culture, mission, and many other factors. C-SCRM activities at each of the three levels include the production of different high-level C-SCRM deliverables.

- At Level 1 (Enterprise), the overall C-SCRM strategy, policy, and implementation plan set the tone, governance structure, and boundaries for how C-SCRM is managed across the enterprise and guide C-SCRM activities performed at the mission and business process levels.

[18] Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.
[19] Additional information about the concepts depicted in Figure 2-2 can be found in [NIST SP 800-39].

- At Level 2 (Mission and Business Process), the mid-level C-SCRM strategies, policies, and implementation plans assume the context and direction set forth at the enterprise level and tailor it to the specific mission and business process.
- At Level 3 (Operational), the C-SCRM plans provide the basis for determining whether an information system meets business, functional, and technical requirements and includes appropriately tailored controls. These plans are heavily influenced by the context and direction provided by Level 2.

Figure 2-4 provides an overview of the multilevel risk management structure and the associated strategies, policies, and plans developed at each level. Refer to Sections 2.3.1 through 2.3.5 for a more in-depth discussion of the specific activities at each level.

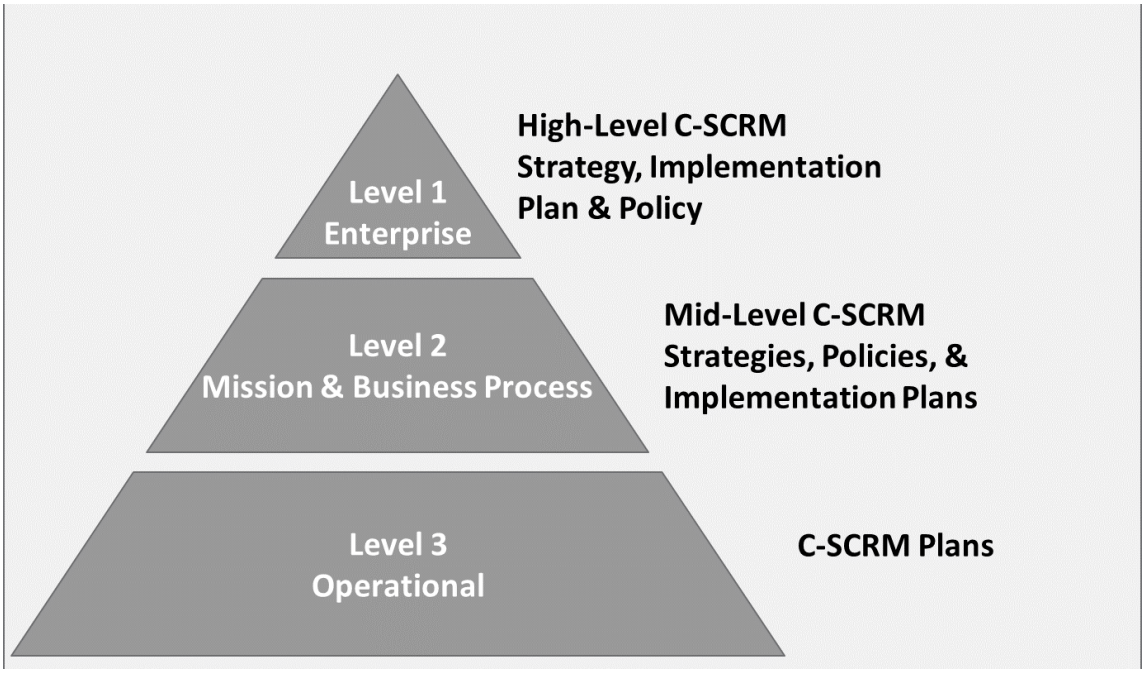

Fig. 2-4: C-SCRM Documents in Multilevel Enterprise-wide Risk Management

2.3.1. Roles and Responsibilities Across the Three Levels

Implementing C-SCRM requires enterprises to establish a coordinated team-based approach and a shared responsibility model to effectively manage cybersecurity risks throughout the supply chain. Enterprises should establish and adhere to C-SCRM-related policies, develop and follow processes (often cross-enterprise in nature), and employ programmatic and technical mitigation techniques. The coordinated team approach, either ad hoc or formal, enables enterprises to 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. The C-SCRM team should work together to make decisions and take actions deriving from the input and involvement of multiple perspectives and expertise. The team leverages but does not replace those C-SCRM responsibilities and processes that should be specifically assigned to an individual enterprise or disciplinary area. Effective implementations of C-SCRM often include the adoption of a shared responsibility model, which

distributes responsibilities and accountabilities for C-SCRM-related activities and risk across a diverse group of stakeholders. Examples of C-SCRM activities in which enterprises benefit from a multidisciplinary approach include developing a strategic sourcing strategy, incorporating C-SCRM requirements into a solicitation, and determining options for 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 enterprise's critical processes, such as information security, procurement, enterprise risk management, engineering, software development, IT, legal, and HR. To aid in C-SCRM, these individuals should provide expertise in enterprise processes and practices specific to their discipline area and 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 enterprise's existing enterprise risk management function, grown as part of an enterprise's cybersecurity risk management function, or operate out of a different department.

The key to forming multidisciplinary C-SCRM teams is breaking down barriers between otherwise disparate functions within the enterprise. Many enterprises begin this process from the top by establishing a working group or council of senior leaders with representation from the necessary and appropriate functional areas. A charter should be established outlining the goals, objectives, authorities, meeting cadences, and responsibilities of the working group. Once this council is formed, decisions can be made on how to operationalize the interdisciplinary approach at mission and business process and operational levels. This often takes the form of working groups that consist of mission and business process representatives who can meet at more regular cadences and address more operational and tactically focused C-SCRM challenges.

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: Cybersecurity Supply Chain Risk Management Stakeholders[20]

Levels	Level Name	Generic Stakeholder	Activities
1	Enterprise	Executive Leadership: CEO, CIO, COO, CFO, CISO, Chief Technology Officer (CTO), Chief Acquisition Officer (CAO), Chief Privacy Officer (CPO), CRO, etc.	• Define Enterprise C-SCRM strategy. • Form governance structures and operating model. • Frame risk for the enterprise, and set the tone for how risk is managed (e.g., set risk appetite).

[20] Small and mid-sized businesses may not see such a high-degree of differentiation in their C-SCRM stakeholders.

Levels	Level Name	Generic Stakeholder	Activities
			• Define high-level implementation plan, policy, goals, and objectives. • Make enterprise-level C-SCRM Decisions. • Form a C-SCRM PMO.
2	Mission and Business Process	Business Management: Program management [PM], project managers, integrated project team (IPT) members, research and development (R&D), engineering (SDLC oversight), acquisition and supplier relationship management/cost accounting, and other management related to reliability, safety, security, quality, the C-SCRM PMO, etc.	• Develop mission and business process-specific strategy. • Develop policies and procedures, guidance, and constraints. • Reduce vulnerabilities at the onset of new IT projects and/or related acquisitions. • Review and assess system, human, or organizational flaws that expose business, technical, and acquisition environments to cyber threats and attacks. • Develop C-SCRM implementation plan(s). • Tailor the enterprise risk framework to the mission and business process (e.g., set risk tolerances). • Manage risk within mission and business processes. • Form and/or collaborate with a C-SCRM PMO. • Report on C-SCRM to Level 1 and act on reporting from Level 3.

Levels	Level Name	Generic Stakeholder	Activities
3	Operational	Systems Management: Architects, developers, system owners, QA/QC, testing, contracting personnel, C-SCRM PMO staff, control engineer and/or control system operator, etc.	• Develop C-SCRM plans. • Implement C-SCRM policies and requirements. • Adhere to constraints provided by Level 1 and Level 2. • Tailor C-SCRM to the context of the individual system, and apply it throughout the SDLC. • Report on C-SCRM to Level 2.

The C-SCRM process should be carried out across the three risk management levels with the overall objective of continuous improvement of the enterprise's risk-related activities and effective inter- and intra-level communication, thus integrating both strategic and tactical activities among all stakeholders with a shared interest in the mission and business success of the enterprise. Whether addressing a component, system, process, mission process, or 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. Figure 2-5 illustrates the relationship between key C-SCRM documents across the three levels.

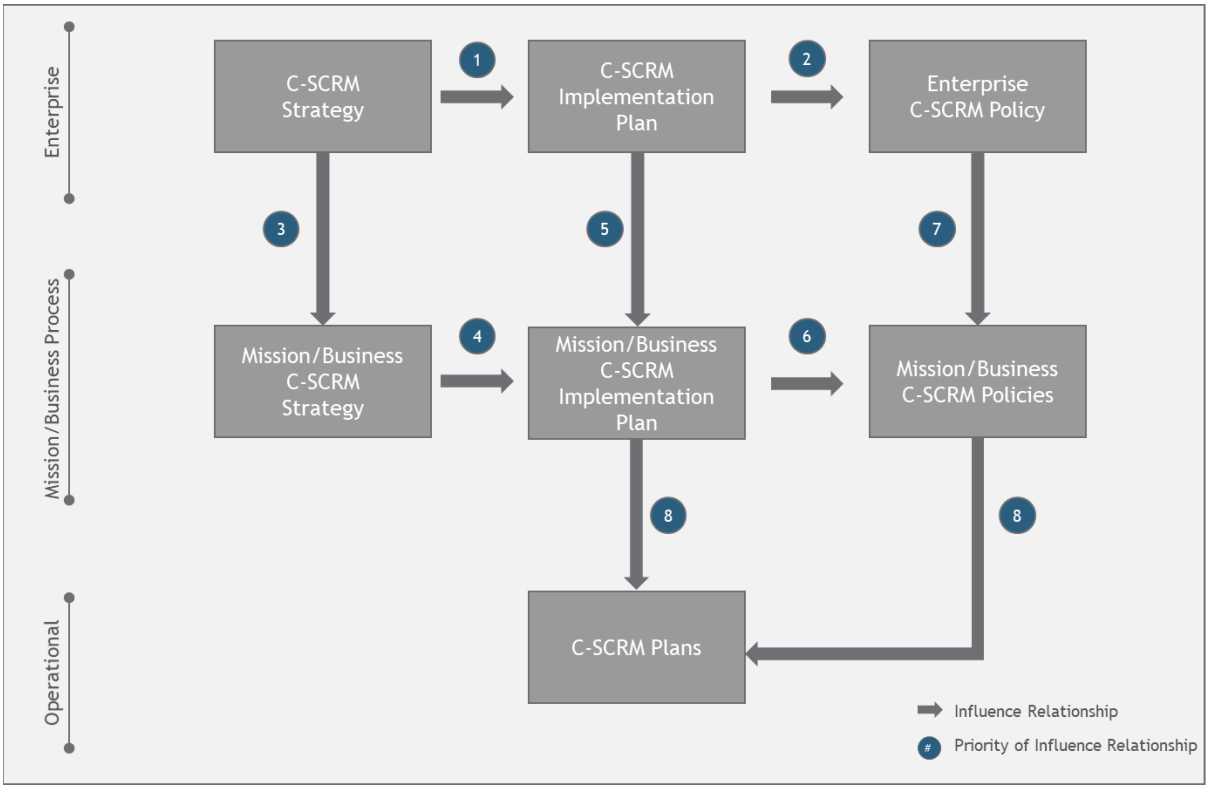

Fig. 2-5: Relationship Between C-SCRM Documents

The next few sections provide example roles and activities at each level. Because every enterprise is different, however, activities may be performed at different levels than listed and as individual enterprise context requires.

> Appendix A provides a number of mission and business C-SCRM controls that organizations can utilize in a tailored capacity to help guide Level 1, Level 2, and Level 3 C-SCRM activities. Note that 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 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.

2.3.2. Level 1 – Enterprise

Effective C-SCRM requires commitment, direct involvement, and ongoing support from senior leaders and executives. Enterprises should designate the responsibility for leading agency-wide SCRM activities to an executive-level individual, office (supported by an expert staff), or group (e.g., a risk board, executive steering committee, or executive leadership council) regardless of an agency's specific organizational structure. Because cybersecurity risks throughout the supply chain can be present across every major business line, enterprises should ensure that C-SCRM

roles and responsibilities are defined for senior leaders who participate in supply chain activities (e.g., acquisition and procurement, information security, information technology, legal, program management, and supply chain and logistics). Without establishing executive oversight of C-SCRM activities, enterprises are limited in their ability to make risk decisions across the organization about how to effectively secure their product and services.

Level 1 (Enterprise) sets the tone and direction for enterprise-wide C-SCRM activities by providing an overarching C-SCRM strategy, a C-SCRM policy, and a High-level Implementation Plan that shapes how C-SCRM is implemented across the enterprise. Within Level-1, governance structures are formed to enable senior leaders and executives to collaborate on C-SCRM with the risk executive (function), make C-SCRM decisions, delegate decisions to Level 2 and Level 3, and prioritize enterprise-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 enterprise. 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 Level 2 and Level 3.

Ownership and accountability for cybersecurity risks in the supply chain ultimately lie with the head of the organization.

- Decision-makers are informed by an organization's risk profile, risk appetite, and risk tolerance levels. Processes should address when and how the escalation of risk decisions needs 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.

C-SCRM requires accountability, commitment, oversight, direct involvement, and ongoing support from senior leaders and executives. Enterprises should ensure that C-SCRM roles and responsibilities are defined for senior leaders who participate in supply chain activities (e.g., acquisition and procurement, information security, information technology, legal, program management, and supply chain and logistics). At Level 1, an executive board is typically responsible for evaluating and mitigating all risks across the enterprise. This is generally achieved through an Enterprise Risk Management (ERM) council. Effective C-SCRM gathers perspectives from leaders, all generally within the ERM council – 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) – and informs advice and recommendations from the CIO and CISO to the executive board.

CIOs and/or CISOs may form a C-SCRM oriented-body to provide in-depth analysis to inform the executive board's ERM council. The C-SCRM council serves as a forum for setting priorities and managing cybersecurity risk in the supply chain for the enterprise. The C-SCRM council or

other C-SCRM-oriented body are responsible for developing the C-SCRM enterprise-wide strategy. The C-SCRM strategy makes explicit the enterprise's assumptions, constraints, risk tolerances, and priorities/trade-offs as established by the ERM council. C-SCRM is integrated into the organization's overall enterprise risk management through the CIO and/or CISO membership within the executive board's ERM council.

These leaders are also responsible and accountable for developing and promulgating a holistic set of policies that span the enterprise's mission 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 should establish a C-SCRM PMO or other dedicated C-SCRM-related function to drive C-SCRM activities and serve as a fulcrum for coordinated, C-SCRM-oriented services and guidance to the enterprise. Leaders should also clearly articulate the lead roles at the mission and business process level that are responsible and accountable for detailing action plans and executing C-SCRM activities. Enterprises should consider that without establishing executive oversight of C-SCRM activities, enterprises are limited in their ability to make risk decisions across the organization about how to effectively secure their product and services.

The C-SCRM governance structures and operational model dictate the authority, responsibility, and decision-making power for C-SCRM and define *how* C-SCRM processes are accomplished within the enterprise. The best C-SCRM governance and operating model is one that meets the business and functional requirements of the enterprise. For example, an enterprise facing strict budgetary constraints or stiff C-SCRM requirements may consider governance and operational models that centralize the decision-making authority and rely on a C-SCRM PMO to consolidate responsibilities for resource-intensive tasks, such as vendor risk assessments. In contrast, enterprises that have mission and business processes governed with a high degree of autonomy or that 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 enterprise. C-SCRM framing is the process by which the enterprise makes explicit the assumptions about cybersecurity risks throughout the supply chain (e.g., threats, vulnerabilities, risk impact,[21] risk likelihood), constraints (e.g., enterprise policies, regulations, resource limitation, etc.), appetite and tolerance, and priorities and trade-offs that guide C-SCRM decisions across the enterprise. The risk framing process provides the inputs necessary to establish the C-SCRM strategy that dictates how the enterprise plans to assess, respond to, and monitor cybersecurity risks throughout the supply chain. A high-level implementation plan should also be developed to guide the execution of the enterprise's C-SCRM strategy. The risk framing process is discussed in further detail in Appendix C.

Informed by the risk framing process and the C-SCRM strategy, Level 1 provides the enterprise's C-SCRM policy. The C-SCRM policy establishes the C-SCRM program's purpose, outlines the enterprise's C-SCRM responsibilities, defines and grants authority to C-SCRM roles across the enterprise, and outlines applicable C-SCRM compliance and enforcement expectations

[21] Risk impact refers to 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 [800-53 R5].

and processes. Appendix C 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 cybersecurity risks throughout the supply chain. Level 1 risk assessments may be based on the enterprise's Level 1 Frame step (i.e., assumptions, constraints, appetite, tolerances, priorities, and trade-offs) or may be aggregated enterprise-level assumptions based on risk assessments that are completed across multiple mission and business processes. For example, a Level 1 risk assessment may assess the exposure to threats to enterprise objectives that arise through supply chain products or services. Level 1 risk assessments may also aim to aggregate and recontextualize risk assessments completed at Level 2 to describe risk scenarios against the enterprise's primary objectives.

Reporting plays an important role in equipping Level 1 decision-makers with the context necessary to make informed decisions on how to manage cybersecurity risks throughout the supply chain. Reporting should focus on enterprise-wide trends and include coverage of the extent to which C-SCRM has been implemented across the enterprise, the effectiveness of C-SCRM, and the conditions related to cybersecurity risks throughout the supply chain. C-SCRM reports should highlight any conditions that require urgent leadership attention and/or action and may benefit from highlighted C-SCRM risk and performance trends over a period of time. Those responsible and accountable for C-SCRM within the enterprise should work with leaders to identify reporting requirements, such as frequency, scope, and format. Reporting should include metrics discussed further in Section 3.5.1.

Level 1 activities ultimately provide the overarching context and boundaries within which the enterprise's mission and business processes manage cybersecurity risks throughout the supply chain. 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.

Note that, in complex enterprises, Level 1 activities may be completed at an enterprise level and at an individual organization level. Enterprise Level 1 activities should shape and guide Organization Level 1 activities.

Additional information can be found in Appendix A of this document and SR-1, SR-3, PM-2, PM-6, PM-7, PM-9, PM-28, PM-29, PM-30, and PM-31 of NIST SP 800-53, Rev. 5.

2.3.3. Level 2 – Mission and Business Process

Level 2 addresses how the enterprise mission and business processes assess, respond to, and monitor cybersecurity risks throughout the supply chain. Level 2 activities are performed in accordance with the C-SCRM strategy and policies provided by Level 1.[22] In this level, process-specific C-SCRM strategies, policies, and implementation plans dictate how the enterprise's C-

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

SCRM goals and requirements are met within each mission and business process. Here, specific C-SCRM program requirements are defined and managed and include cost, schedule, performance, security, and a variety of critical non-functional requirements. These non-functional requirements include concepts such as reliability, dependability, safety, security, and quality.

Level 2 roles include representatives of each mission and business process, such as program managers, research and development, and acquisitions/procurement. Level 2 C-SCRM activities address C-SCRM within the context of the enterprise's 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. In order to further develop the high-level Enterprise Strategy and Implementation Plan, different mission areas or business lines within the enterprise may need to generate their own tailored mission and business-level strategy and implementation plan, and they should ensure that C-SCRM execution occurs within the constraints defined by higher level C-SCRM strategies and in conformance C-SCRM policies. To facilitate the development and execution of Level 2 Strategy and Implementation plans, enterprises may benefit from forming a committee with representation from each mission and business process. Coordination and collaboration between the mission and business processes can help drive risk awareness, identify cybersecurity risks throughout the supply chain, and support the development of an enterprise and C-SCRM architecture. 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).

Many threats *to* and *through* the supply chain are addressed at Level 2 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 processes, understanding, integrating, and coordinating C-SCRM activities at this level are critical. Level 2 activities focus on tailoring and applying the enterprise's C-SCRM frame to fit the specific mission and business process threats, vulnerabilities, impacts,[23] and likelihoods. Informed by outputs from Level 1 (e.g., C-SCRM strategy), mission and business processes will adopt a C-SCRM strategy that tailors the enterprise's overall strategy to a specific mission and business process. At Level 2, the enterprise may also issue mission and business process-specific policies that contextualize the enterprise's policy for the process.

In accordance with the C-SCRM strategy, enterprise 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 within the mission and business process. Within the C-SCRM implementation plans, the mission and business process will specify C-SCRM roles, responsibilities, implementation milestones, dates, and processes for monitoring and reporting. Appendix D of this document

[23] These impacts refer to the effects 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 [SP 800-53, Rev. 5].

provides example templates for the C-SCRM Strategy, Implementation Plan, and 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 occur as a result of primary dependencies on the supply chain or secondary dependencies on individual information systems or other mission and business processes. For example, risk exposure may arise due to a supplier providing critical system components or services to multiple information systems on which critical processes depend. Risk may also arise from vendor-sourced products and services unrelated to information systems, as well as the roles that these products and services play in the overall mission and business process objectives. Enterprises should consider non-traditional sources of cybersecurity risks throughout the supply chain. These risks may circumvent or escape C-SCRM processes, such as those arising from the use of open source software. Enterprises should establish policies and controls to manage non-traditional cybersecurity risks throughout the supply chain.

Reporting at Level 2 plays an important role in equipping mission and business process leaders with the context necessary to manage C-SCRM within the scope of their mission and business processes. Topics covered at Level 2 will reflect those covered at Level 1 but should be reshaped to focus on the specific mission and business process that they correspond to. Level 2 reporting should include metrics that demonstrate the mission and business process performance in contrast to the enterprise-defined risk appetite and risk tolerance statements defined at Level 1 and Level 2. Reporting requirements should be defined to fit the needs of leaders in mission and business processes and at Level 1.

Outputs from Level 2 activities will significantly impact how C-SCRM activities are carried out at 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 at Level 3. Level 2 outputs should also be used to iteratively influence and further refine Level 1 outputs.

Additional information can be found in Appendix A of this document and SR-1, SR-3, SR-6, PM-2, PM-6, PM-7, PM-30, PM-31, and PM-32 of NIST SP 800-53, Rev. 5.

2.3.4. Level 3 – Operational

Level 3 is comprised of personnel responsible and accountable for operational activities, including conducting procurements and executing system-related C-SCRM activities as part of the enterprise's SDLC, which includes research and development, design, manufacturing, delivery, integration, operations and maintenance, and the disposal/retirement of systems. These personnel include system owners, contracting officers, contracting officer representatives, architects, system engineers, information security specialists, system integrators, and developers. These personnel are responsible for developing C-SCRM plans that address the management, implementation assurance, and monitoring of C-SCRM controls (to include those applicable to external parties, such as contractors) and the acquisition, development, and sustainment of systems and components across the SDLC to support mission and business processes. In

enterprises where a C-SCRM PMO has been established, activities such as product risk assessments may be provided as a centralized, shared service.

Within Level 3, outputs provided by C-SCRM activities completed at Level 1 and Level 2 prepare the enterprise 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 assumptions, constraints, risk appetite and tolerance, priorities, and trade-offs defined by Level 1 and Level 2. C-SCRM plans dictate how C-SCRM activities are integrated into all systems in the SDLC: 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 processes.

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 enterprise 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 supply chain cybersecurity threats exploiting an operational-level vulnerability (e.g., in a system or system component). Where applicable, these risk assessments should be informed by risk assessments completed in Level 1 and Level 2. In response to determining risk, enterprises 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 the Level 1 and Level 2 and information system-specific controls at Level 3.

Reporting at Level 3 should focus on the C-SCRM's implementation, efficiency, effectiveness, and the overall level of exposure to cybersecurity risks in the supply chain for the particular system. System-level reporting should provide system owners with tactical-level insights that enable them to make rapid adjustments and respond to risk conditions. Level 3 reporting should include metrics that demonstrate performance against the enterprise risk appetite statements and risk tolerance statements defined at Levels 1, 2, and 3.

A critical 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, critical system personnel, related laws, regulations, policies, and contingency plan. In C-SCRM, continuous hygiene is critical, and the C-SCRM plan is a living document that should be maintained and used as the reference for the continuous monitoring of implemented C-SCRM controls. C-SCRM 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, enterprises 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.

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

Additional information can be found in Appendix A of this document and SR-1, SR-2, SR-6, PL-2, PM-31, and PM-32 of NIST SP 800-53, Rev. 5.

2.3.5. C-SCRM PMO

A variety of operating models (e.g., centralized, decentralized, hybrid) facilitate C-SCRM activities across the enterprise and its mission and 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 mission and business processes. Mission and business processes are then responsible for selecting and requesting services from the C-SCRM PMO as part of their responsibilities to meet the enterprise's C-SCRM goals and objectives. There are a variety of beneficial services that a PMO may provide:

- Advisory services and subject matter expertise
- Chair for internal C-SCRM working groups, council, or other coordination bodies
- Centralized hub for tools, job aids, awareness, and training templates
- Supplier and product risk assessments
- Liaison to external stakeholders
- Information-sharing management (e.g., intra department/agency and 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 enterprise and its mission and business processes. A C-SCRM PMO may include or report to a dedicated executive-level official responsible and accountable for overseeing C-SCRM activities across the enterprise. A C-SCRM PMO should consist of dedicated personnel or include matrixed representatives with responsibilities for C-SCRM from several of the enterprise's processes, including information security, procurement, risk management, engineering, software development, IT, legal, and HR. Regardless of whether a C-SCRM PMO sits at Level 1 or Level 2, it is critical that the C-SCRM PMO include cross-disciplinary representation.

The C-SCRM PMO responsibilities may include providing services to the enterprise's leaders that help set the tone for how C-SCRM is applied throughout the enterprise. The C-SCRM PMO may provide SME support to guide Level 1 stakeholders through the risk framing process, which includes establishing the enterprise appetite and tolerance for cybersecurity risks throughout the supply chain. In addition, accountable risk executives may delegate the responsibility of drafting the enterprise's C-SCRM strategy and policy to the PMO. C-SCRM PMOs may also coordinate C-SCRM information-sharing internally or with external entities. 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 view of cybersecurity risks throughout the supply chain.

At Level 2, the C-SCRM PMO may develop C-SCRM starter kits that contain a base strategy and a set of policies, procedures, and guidelines that 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 enterprise 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 Level 1 and Level 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 enterprises an opportunity to capitalize on specialized skill sets within a consolidated team that offers high-quality C-SCRM services to the rest of the enterprise. By centralizing risk assessment services, enterprises may achieve a level of standardization not otherwise possible (e.g., in a decentralized model). Enterprises may also realize cost efficiencies in cases where PMO resources are dedicated to C-SCRM activities versus resources in decentralized models that may perform multiple roles in addition to C-SCRM responsibilities.

A C-SCRM PMO model will typically favor larger, more complex enterprises that require the standardization of C-SCRM practices across a disparate set of mission and business processes. Ultimately, enterprises should select a C-SCRM operating model that is applicable and appropriate relative to their available resources and context.

Key Takeaways[24]

Business Case for C-SCRM. C-SCRM provides enterprises with a number of benefits, such as an understanding of critical systems, the reduced likelihood of supply chain compromise, operational and enterprise efficiencies, fewer product quality and security issues, and more reliable and trustworthy supplied services.

Cybersecurity Risk in Supply Chains. The potential for harm or compromise arising from a relationship with suppliers, their supply chains, and their supplied products or services materialize when a human or non-human threat successfully exploits a vulnerability tied to a system, product, service, or the supply chain ecosystem.

Multilevel, Multidisciplinary C-SCRM. As described in [NIST SP 800-39], multilevel risk management is the purposeful execution and continuous improvement of cybersecurity supply chain risk management activities at the enterprise (e.g., CEO, COO), mission and business process (e.g., business management, R&D), and operational (e.g., systems management) levels. Each level contains stakeholders from multiple disciplines (e.g., information security, procurement, enterprise risk management, engineering, software development, IT, legal, HR, etc.) that collectively execute and continuously improve C-SCRM

C-SCRM PMO. A dedicated office known as a C-SCRM PMO may support the enterprise's C-SCRM activities by providing support products (e.g., policy templates) and services (e.g., vendor risk assessments) to the rest of the enterprise. A C-SCRM PMO may provide support across the three levels and sit at Level 1 or Level 2, depending on the enterprise.

C-SCRM is a Life Cycle Process. C-SCRM activities should be integrated and executed throughout the applicable enterprise life cycle processes (e.g., SDLC). For example in systems, cybersecurity supply chain risks can and do materialize during operations and maintenance phases. Organizations should ensure that appropriate C-SCRM activities are in place to assess, respond to, and monitor cybersecurity supply chain risks on a continuous basis.

[24] Key takeaways describe key points from the section text. Refer to the Glossary in Appendix H for definitions.

3. CRITICAL SUCCESS FACTORS

To successfully address evolving cybersecurity risks throughout the supply chain, enterprises need to engage multiple internal processes and capabilities, communicate and collaborate across enterprise levels and mission areas, and ensure that all individuals within the enterprise understand their role in managing cybersecurity risks throughout the supply chain. Enterprises need strategies for communicating, determining how best to implement, and monitoring the effectiveness of their supply chain cybersecurity controls and practices. In addition to internally communicating cybersecurity supply chain risk management controls, enterprises should engage with peers to exchange C-SCRM insights. These insights will aid enterprises 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 enterprise processes and capabilities in making C-SCRM successful. While this publication has chosen to highlight these critical success factors, this represents a non-exhaustive set of factors that contribute to an enterprise's successful execution of C-SCRM. Critical success factors are fluid and will evolve over time as the environment and the enterprise's own capability advances.

3.1. C-SCRM in Acquisition[25]

Integrating C-SCRM considerations into acquisition activities within every step of the procurement and contract management life cycle process is essential to improving management of cybersecurity risks throughout the supply chain. This life cycle begins with a purchaser identifying a need and includes the processes to plan for and articulate requirements, conduct research to identify and assess viable sources of supply, solicit bids, evaluate offers to ensure conformance with C-SCRM requirements, and assess C-SCRM risks associated with the bidder and the proposed product and/or service. After contract award, ensure that the supplier satisfies the terms and conditions articulated in the contractual agreement and that the products and services conform as expected and required. Monitoring for changes that may affect cybersecurity risks in the supply chain should occur throughout the life cycle and may trigger reevaluation of the original assessment or require a mitigation response.

Enterprises rely heavily on commercial products and outsourced services to perform operations and fulfill their mission and business objectives. However, it is important to highlight that products and services can also be obtained outside of the procurement process, as is the case with open source software, relying on an in-house provider for shared services, or by repurposing an existing product to satisfy a new need. C-SCRM must also be addressed for these other "acquiring" processes.

In addition to addressing cybersecurity risks throughout the supply chain and performing C-SCRM activities during each phase of the acquisition process, enterprises should develop and execute an acquisition strategy that drives reductions in their overall risk exposure. By applying such strategies, enterprises can reduce cybersecurity risks throughout the supply chain, within specific procurement processes, and for the overall enterprise. Enterprises will aid, direct, and

[25] Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

inform efforts to realize targeted risk-reducing outcomes by adopting acquisition policies and processes that integrate C-SCRM into acquisition activities.

Additionally, by adopting C-SCRM controls aligned to an industry-recognized set of standards and guidelines (e.g., NIST 800-53, Rev.5; NIST CSF), the enterprise can ensure holistic coverage of cybersecurity risks throughout the supply chain and corresponding C-SCRM practices. C-SCRM controls may apply to different participants of the supply chain to include the enterprise itself, prime contractors, and subcontractors. Because enterprises heavily rely on prime contractors and their subcontractors to develop and implement ICT/OT products and services, those controls implemented within the SDLC are likely to flow down to subcontractors. Establishing C-SCRM controls applicable throughout the supply chain and the SDLC will aid the enterprise in establishing a common lexicon and set of expectations with suppliers and sub-suppliers to aid all participants in managing cybersecurity risks throughout the supply chain.

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

An enterprise's C-SCRM Strategy and Implementation Plan guides the enterprise toward the achievement of long-term, sustainable reductions in exposure to cybersecurity risks throughout the supply chain. As a core part of the C-SCRM Strategy and Implementation Plan, enterprises should address how this risk is managed throughout the acquisition process.

Cybersecurity risks in the supply chain include those arising from the supplier's enterprise, products, services, and 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:

- 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 that necessary provision and protections are in place
- Leveraging an external shared service provider or utilizing the C-SCRM PMO to provide supplier, product, and/or service assessment activities as a shared service to other internal processes, including acquisition
- Conducting due diligence to inform determinations about a bidder's responsibility and to identify and assess bidders' risk posture or risk associated with a given product or service
- Obtaining open source software from vetted and approved libraries
- Including C-SCRM criteria in source selection evaluations
- Establishing and referencing a list of prohibited suppliers, if appropriate, per applicable regulatory and legal references
- Establishing and procuring from an approved products list or list of preferred or qualified suppliers who have demonstrated conformance with the enterprise's security requirements through a rigorous process defined by the enterprise or another acceptable qualified list program activity [CISA SCRM WG3]

- Ensuring that products, including software or logic-bearing products (i.e., hardware), are supplied with a software bill of materials that complies with appropriate agency-approved protocols

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, enterprise leaders should promote the value and importance of C-SCRM within acquisitions and ensure that sufficient, dedicated funding is in place for necessary activities. Doing so will help enterprises ensure responsibility for program or business processes and accountability for progress toward the attainment of results. Enterprises should build sufficient time into acquisition and project activities to ensure that C-SCRM activities can be completed. Enterprises should also assign roles and responsibilities, some of which will be cross-enterprise 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 that roles and responsibilities are understood and executed in alignment with leader expectations.

The enterprise'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 both realistic and achievable. This baseline starting point also serves as a marker by which performance progress and outcomes can be tracked and assessed.

A critical first step is to ensure that there is a current and accurate inventory of the enterprise's supplier relationships, contracts, and any products or services those suppliers provide. This information allows for a mapping of these suppliers into strategically relevant groupings as determined by the organization. For example, an assessment of these suppliers might result in groupings of multiple categories (e.g., "strategic/innovative," "mission-critical," "sustaining," or "standard/non-essential"). This segmentation facilitates further analysis and understanding of the exposure to cybersecurity risks throughout the supply chain and helps to focus attention and assign priority to those critical suppliers of the most strategic or operational importance to the enterprise and its mission and business processes. It is useful to identify which products and services require a higher level of confidence in risk mitigation and 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 Appendix A of this document, [NISTIR 8179], and SA-1, SA-2, SA-4, SR-5, SR-13 of NIST SP 800-53, Rev. 5.

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

When conducting a procurement, enterprises should designate experts from different subject matter areas to participate in the acquisition process as members of the Acquisition Team and/or Integrated Project Team.[26] This includes program officials, personnel with technical and security expertise, and representatives from supply and procurement communities. While procurement requirements address and are tailored to a specific purpose and ensuring that compliance mandates are met, contextual factors such as mission criticality, the sensitivity of data, and the

[26] An Integrated Project Team is equivalent to the acquisition team, as defined by the FAR

operational environment must also be considered to effectively address cybersecurity risk in supply chains.

This contextual basis sets the stage for the Acquisition Team to effectively gauge their tolerance for risk as it pertains to a specific procurement requirement and determine which of the C-SCRM controls described in this document 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 critical factor in procurement decisions. For this reason, when purchasing ICT/OT-related products or services, enterprises should avoid using a "lowest price, technically acceptable" (LPTA) source selection process.

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 and develop requirements, perform market analysis, complete procurement, ensure compliance, and monitor performance for changes that affect C-SCRM risk status) as described in [NISTIR 7622]. This includes ensuring that cybersecurity risks throughout the supply chain are addressed when making ICT/OT-related charge card purchases.

During the 'plan procurement' step, the need for and the criticality of the good or service to be procured needs to be identified, along with a description of the factors driving the determination of the need and level of criticality as this informs how much risk may be tolerated, who should be involved in the planning, and the development of the specific requirements that will need to be satisfied. This activity is typically led by the acquirer mission and business process owner or a designee in collaboration with the procurement official or contracting officer representative

During the planning phase, the enterprise should develop and define requirements to address cybersecurity risks throughout the supply chain in addition to specifying performance, schedule, and cost objectives. This process is typically initiated by the acquirer mission and business process owner or a designee in collaboration with the procurement official and other members of the C-SCRM team.

With requirements defined, enterprises will typically complete a market analysis for potential suppliers. Market research and analysis activities 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. Enterprises 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 enterprise may consider the market concentration for the sought-after product or service as a means of identifying interdependencies within the supply chain. The enterprise may also use a request for information (RFIs), sources sought notice (SSNs), and/or due diligence questionnaires for the initial screening and collection of evidence from potential suppliers. Enterprises 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 enterprise will complete the procurement step by releasing a statement of work (SOW), performance work statement (PWS), or statement of objective (SOO) for the release of a request for proposal (RFP) or request for quotes (RFQ). Any bidders responding to the RFP or RFQ should be evaluated against relevant, critical 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 enterprise, 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, appropriate information system owners, and technical experts. Prior to purchase, enterprises should identify and assess the quality of the product or system components, vulnerability(s) authenticity, and other relevant cybersecurity-supply chain risk factors and complete this risk assessment prior to deployment.

Once the contract is executed, the enterprise should monitor for changes that alter its exposure to cybersecurity risks throughout the supply chain. Such changes may include internal enterprise or system changes, supplier operational or structural changes, product updates, and geopolitical or environmental changes. Contracts should include provisions that provide grounds for termination in cases where there are changes to cybersecurity supply chain risk that cannot be adequately mitigated to within acceptable levels. Finally, enterprises should continuously apply lessons learned and collected during the acquisition process to enhance their ability to assess, respond to, and monitor cybersecurity risks throughout the supply chain.

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

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 or Develop Requirements	Identify relevant C-SCRM controls or requirements	Identify relevant C-SCRM controls or requirements	Identify relevant C-SCRM controls or requirements
Perform Market Analysis	Initial Risk Assessment (e.g., due diligence questionnaires)	Initial Risk Assessment (e.g., due diligence questionnaires)	Research product options and risk factors
Solicit Bids/ Complete Procurement	Confirm C-SCRM Requirements Met Complete Risk Assessment	Confirm C-SCRM Requirements Met Complete Risk Assessment	Pre-deployment Risk Assessment

Procurement Process	Service Risk Assessment	Supplier Risk Assessment	Product Risk Assessment
Operate and Maintain	Continuous Risk Monitoring	Continuous Risk Monitoring	Continuous Risk Monitoring

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

To ensure the effective and continued management of cybersecurity risks across the supply chain and throughout the acquisition life cycle, contractual agreements and contract management should include:

- The satisfaction of applicable security requirements in contracts and mechanisms as a qualifying condition for award;
- Flow-down control requirements to subcontractors, if and when applicable, including C-SCRM performance objectives linked to the method of inspection in a Quality Assurance Surveillance Plan or equivalent method for monitoring performance;
- The periodic revalidation of supplier adherence to security requirements to ensure continual compliance;
- Processes and protocols for communication and the reporting of information about vulnerabilities, incidents, and other business disruptions, including acceptable deviations if the business disruption is deemed serious and baseline criteria to determine whether a disruption qualifies as serious; and
- Terms and conditions that address the government, supplier, and other applicable third-party roles, responsibilities, and actions for responding to identified supply chain risks or risk incidents 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 revalidation methods, such as requisite certifications, site visits, third-party assessments, or self-attestation. The type and rigor of the required methods should be commensurate with 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, which demonstrates the enhanced overlay of C-SCRM into the [NIST SP 800-39] Risk Management Process. In addition, enterprises should refer to and follow the acquisition and 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 Appendix A of this document and 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 of NIST SP 800-53, Rev. 5.

3.2. Supply Chain Information Sharing

Enterprises are continuously exposed to risk originating from their supply chains. An effective information-sharing process helps to ensure that enterprises can gain access to information that is critical to understanding and mitigating cybersecurity risks throughout the supply chain and also share relevant information with others that may benefit from or require awareness of these risks.

To aid in identifying, assessing, monitoring, and responding to cybersecurity risks throughout the supply chain, enterprises should build information-sharing processes and activities into their C-SCRM programs. This may include establishing information-sharing agreements with peer enterprises, business partners, and suppliers. By exchanging Supply Chain Risk Information (SCRI) within a sharing community, enterprises can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats that the enterprise may face. Additionally, the sharing of SCRI allows enterprises to better detect campaigns that target specific industry sectors and institutions. However, the enterprise should be sure that information sharing occurs through formal sharing structures, such as Information Sharing and Analysis Centers (ISACs). Informal or unmanaged information sharing can expose enterprises to potential legal risks.

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

NIST SP 800-150 describes key practices for establishing and participating in SCRI-sharing relationships, including:

- Establish information-sharing goals and objectives that support business processes and security policies
- Identify existing internal sources of SCRI
- Specify the scope of information-sharing activities[27]
- 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 SCRI
- Proactively establish SCRI-sharing agreements
- Protect the security and privacy of sensitive information

[27] The scope of information sharing activities should include the data classification level that was approved at the most recent risk assessment for a supplier and the data types that were approved for that supplier. For example, if an assessment was performed for data at a certain classification level (e.g., Business Confidential) and the scope of the engagement changes to include data at a new classification level (e.g., restricted), the risk assessment needs to be refreshed.

- Provide ongoing support for information-sharing activities

As shown in Table 3-2, below, SCRI describes or identifies the cybersecurity supply chain relevant characteristics and risk factors associated with a product, 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 by the metadata that will facilitate an assessment of a level of confidence in and credibility of the information. Enterprises should follow established processes and procedures that describe whether and when the sharing or reporting of certain information is mandated or voluntary and if there are any necessary requirements to adhere to regarding information handling, protection, and classification.

Table 3-2: Supply Chain Characteristics and Cybersecurity Risk Factors Associated with a Product, Service, or Source of Supply[28]

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)[29] • Market alternatives to the source • Provenance and pedigree of components • Supply chain relationships and locations	• Threat information includes indicators (system artifacts or observables associated with an attack), tactics, techniques, and procedures (TTPs) • Security alerts or threat intelligence reports • Implications to national security, homeland security, national critical infrastructure, or the processes associated with the 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 enterprise's operations or mission and the likelihood of a potential impact, harm, or the exploitability of a system • The capacity to mitigate risks is identified

[28] Supply Chain Characteristics and Cybersecurity Risk Factors Associated with a Product, Service, or Source of Supply is non-exhaustive.
[29] Special 301 Report, prepared annually by the Office of the United States Trade Representative (USTR), provides supplemental guidance for intellectual property handling (https://ustr.gov/issue-areas/intellectual-property/special-301).

- Potential risk factors, such as geopolitical, 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

3.3. C-SCRM Training and Awareness

Numerous individuals within the enterprise contribute to the success of C-SCRM. These may include information security, procurement, risk management, engineering, software development, IT, legal, HR, and program managers. Examples of these groups' contributions include:

- 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 or review 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 the use of open source components.
- Software developers ensure that software weaknesses and vulnerabilities are identified and addressed as early as possible, including testing and fixing code.
- Shipping and receiving ensures that boxes containing critical components have not been tampered with en route or at the warehouse.
- Project managers ensure that project plans are developed and include C-SCRM considerations as part of the project plan and execution.

Everyone within an enterprise, including the end users of information systems, has a role in managing cybersecurity risks throughout the supply chain. The enterprise should foster an overall culture of security that includes C-SCRM as an integral part. The enterprise 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 enterprise should receive appropriate training to enable them to understand the importance of C-SCRM to their enterprise, their specific roles and responsibilities, and as it relates to processes and procedures for reporting incidents. This training can be integrated into the overall cybersecurity awareness training. Enterprises should define baseline training requirements at a broad scope within Level 1, and those requirements should be tailored and refined based on the specific context within Level 2 and Level 3.

Those individuals who have more significant roles in managing cybersecurity risks throughout the supply chain should receive tailored C-SCRM training that helps them understand the scope of their responsibilities, the specific processes and procedure implementations for which they are responsible, and the actions to take in the event of an incident, disruption, or another C-SCRM-related event. The enterprises should establish specific role-based training criteria and develop role-specific C-SCRM training to address C-SCRM roles and responsibilities. The enterprise may also consider adding C-SCRM content into preexisting role-based training for some specific roles. Refer to the Awareness and Training controls in Section 4.5 for more detail.

Enterprises are encouraged to utilize the NIST National Initiative for Cybersecurity Education (NICE) Framework[30] as a means of forming a common lexicon for C-SCRM workforce topics. This will aid enterprises 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; Knowledge, Skills, and Abilities (KSAs); and Tasks that describe cybersecurity work.

3.4. C-SCRM Key Practices[31]

Cybersecurity supply chain risk management builds on existing standardized practices in multiple disciplines and an ever-evolving set of C-SCRM capabilities. C-SCRM Key Practices are meant to specifically emphasize and draw attention to a subset of the C-SCRM practices described throughout this publication. Enterprises should prioritize achieving a base-level of maturity in these key practices prior to advancing on to additional C-SCRM capabilities. Enterprises should tailor their implementation of these practices to what is applicable and appropriate given their unique context (e.g., based on available resources and risk profile). C-SCRM Key Practices are described in NIST standards and guidelines, such as [NISTIR 8276], and other applicable national and international standards. C-SCRM Practices include integrating C-SCRM across the enterprise; establishing a formal program; knowing and managing critical products, services, and suppliers; understanding an enterprise's supply chain; closely collaborating with critical suppliers; including critical suppliers in resilience and improvement activities; assessing and monitoring throughout the supplier relationship; and planning for the full life cycle.

[30] See NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.*

[31] Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

3.4.1. Foundational Practices

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

- Establish a core, dedicated, multidisciplinary C-SCRM Program Management Office and/or C-SCRM team.
- Obtain senior leadership support for establishing and/or enhancing C-SCRM.
- 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 enterprise-wide risk assessment process (in accordance with NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments* [NIST SP 800-30 Rev. 1]).
- Establish an enterprise governance structure that integrates C-SCRM requirements and incorporates these requirements into the enterprise policies.
- Develop a process for identifying and measuring the criticality of the enterprise'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. Supervisors and managers should also ensure that their staff aims to build C-SCRM competencies.
- 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, physical security, and other relevant processes (e.g., Legal, Risk Executive, 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 sufficient 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 Enterprises [NIST SP 800-53, Rev. 5].

- Establish internal checks and balances to ensure compliance with security and quality requirements.
- Establish a supplier management program that includes, for example, guidelines for purchasing from qualified original equipment manufacturers (OEMs)[32] or their authorized distributors and resellers.
- Implement a robust incident management program to successfully identify, respond to, and mitigate security incidents. This program should be capable of identifying the root cause of security incidents, including those that originate from the cybersecurity supply chain.
- Establish internal processes to validate that suppliers and service providers actively identify and disclose vulnerabilities in their products.
- Establish a governance capability for managing and monitoring components of embedded software to manage risk across the enterprise (e.g., SBOMs paired with criticality, vulnerability, threat, and exploitability to make this more automated).

3.4.2. Sustaining Practices

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

- Establish and collaborate with a threat-informed security program.
- Use confidence-building mechanisms, such as third-party assessment surveys, on-site visits, and formal certifications (e.g., ISO 27001) to assess critical supplier security capabilities and practices.
- Establish formal processes and intervals for continuous monitoring and reassessment of suppliers, supplied products and services, and the supply chain itself for potential changes to the risk profile.
- Use the enterprise's understanding of its C-SCRM risk profile (or risk profiles specific to mission and business areas) to define a risk appetite and risk tolerances to empower leaders with delegated authority across the enterprise to make C-SCRM decisions in alignment with the enterprise's mission imperatives and strategic goals and objectives.
- Use a formalized information-sharing function to engage with ISACs, the FASC, and other government agencies to enhance the enterprise's supply chain cybersecurity threat and risk insights and help ensure a coordinated and holistic approach to addressing cybersecurity risks throughout the supply chain that may affect a broader set of agencies, the private sector, or national security.
- Coordinate with the enterprise's cybersecurity program leadership to elevate top C-SCRM Risk Profile risks to the most senior enterprise risk committee.
- Embed C-SCRM-specific training into the training curriculums of applicable roles across the enterprise processes involved with C-SCRM, including information security, procurement, risk management, engineering, software development, IT, legal, and HR.

[32] For purposes of this publication, the term *original equipment manufacturers* is inclusive of *original component manufacturers*.

- Integrate C-SCRM considerations into every aspect of the system and product life cycle, and implement consistent, well-documented, repeatable processes for systems engineering, cybersecurity practices, and acquisition.
- Integrate the enterprise's defined C-SCRM requirements into the contractual language found in agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.
- Include critical 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.
- Define, collect, and report C-SCRM metrics to ensure risk-aware leadership, enable active management of the completeness of C-SCRM implementations, and drive the efficacy of the enterprise's C-SCRM processes and practices.

3.4.3. Enhancing Practices

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

- Automate C-SCRM processes where applicable and practical to drive execution consistency, efficiency, and make available the critical resources required for other critical C-SCRM activities.
- Adopt quantitative risk analyses that apply probabilistic approaches (e.g., Bayesian analysis) to reduce uncertainty about the likelihood and impact of cybersecurity risks throughout the supply chain, optimize the allocation of resources to risk response, and measure return on investment (i.e., response effectiveness).
- 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 risk profile changes before they occur.
- Establish or participate in a community of practice (e.g., Center of Excellence) as appropriate to enhance and improve C-SCRM practices.

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

3.5. Capability Implementation Measurement and C-SCRM Measures

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

- Using a framework, such as NIST CSF to assess their C-SCRM capabilities
- Measuring the progress of their C-SCRM initiatives toward completion

- Measuring the performance of their C-SCRM initiatives toward 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 progress and results that ultimately indicate reductions in risk exposure and improvements in the enterprise's security outcomes.

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

Enterprises can use a framework to baseline their C-SCRM capabilities, such as NIST CSF Implementation Tiers, which provide a useful context for an enterprise 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 that illustrate the progression of capabilities across tiers. The following are examples of how C-SCRM capabilities could be gauged by applying NIST CSF Tiers:

- CSF Tier 1: The enterprise does not understand its exposure to cybersecurity risks throughout the supply chain or its role in the larger ecosystem. The enterprise does not collaborate with other entities or have processes in place to identify, assess, and mitigate cybersecurity risks throughout the supply chain.
- CSF Tier 2: The enterprise understands its cybersecurity risks throughout the supply chain and its role in the larger ecosystem. The enterprise has not internally formalized its capabilities to manage cybersecurity risks throughout the supply chain or its capability to engage and share information with entities in the broader ecosystem.
- CSF Tier 3: The enterprise-wide approach to managing cybersecurity risks throughout the supply chain is enacted via enterprise risk management policies, processes, and procedures. This likely includes a governance structure (e.g., Risk Council) that balances the management of cybersecurity risks throughout the supply chain with other enterprise risks. Policies, processes, and procedures are consistently implemented as intended and continuously monitored and reviewed. Personnel possess the knowledge and skills to perform their appointed cybersecurity supply chain risk management responsibilities. The enterprise has formal agreements in place to communicate baseline requirements to its suppliers and partners. The enterprise understands its external dependencies and collaborates with partners to share information to enable risk-based management decisions within the enterprise in response to events.
- CSF Tier 4: The enterprise 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 enterprise leverages institutionalized knowledge of cybersecurity supply chain risk management with its external suppliers and partners, internally in related functional areas, and at all levels of the enterprise. The enterprise communicates proactively using formal (e.g., agreements) and informal mechanisms to develop and maintain strong relationships with its suppliers, buyers, and

other partners.

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

Table 3-3: Example C-SCRM Practice Implementation Model[33]

Implementation Level	Associated C-SCRM Practices
Foundational	• Establish a C-SCRM PMO • Obtain leadership support for C-SCRM • C-SCRM policies across enterprise-levels • Define C-SCRM hierarchy • C-SCRM governance structure • Well-documented, consistent C-SCRM processes • Establish a C-SCRM aware culture • Quality and reliability program • Integrate C-SCRM into acquisition/procurement policies • Determine FIPS 199 impact levels • Explicit roles for C-SCRM • Adequate and dedicated C-SCRM resources • Defined C-SCRM control baseline • C-SCRM internal checks and balances to assure compliance • Supplier management program • C-SCRM included in an established incident management program • Processes to ensure suppliers disclose vulnerabilities
Sustaining	• Threat-informed security program • Use of third-party assessments, site visits, and formal certification • Formal supplier monitoring program • Defined C-SCRM risk appetite and risk tolerances • Formalized information-sharing processes (e.g., engages w/ FASC) • Regular reporting of C-SCRM risks to executives/ risk committees • 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 • Collaborate with suppliers to improve their cybersecurity practices

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

	• Formally defined, collected, and reported C-SCRM metrics
Enhancing	• C-SCRM process automation • Use quantitative risk analysis • Predictive and adaptive C-SCRM strategies and processes • Establish or participate in a community of practice

3.5.1. Measuring C-SCRM Through Performance Measures

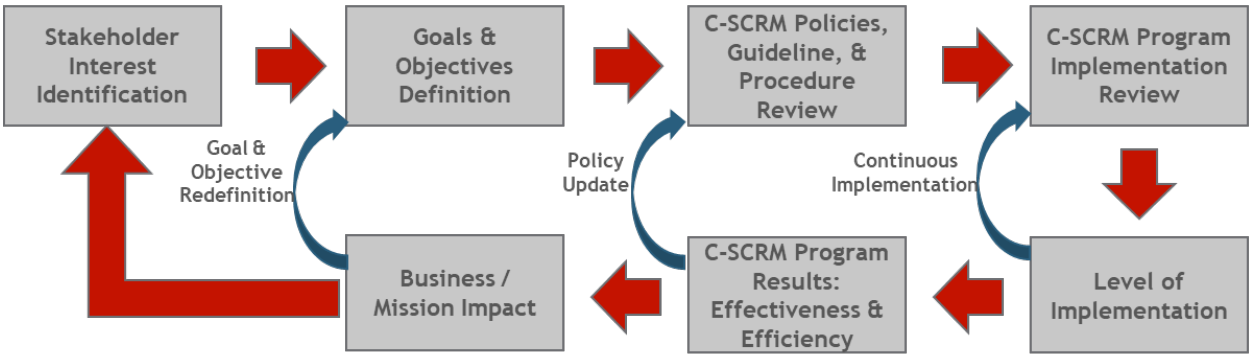

Fig. 3-1: C-SCRM Metrics Development Process

Enterprises typically rely on information security measures to facilitate decision-making and improve performance and accountability in their information security programs. Enterprises can achieve similar benefits within their C-SCRM programs. Additionally, enterprises should report C-SCRM metrics to the board through the ERM process. Figure 3-1 illustrates the process for developing metrics, as outlined in [NIST SP 800-55, Rev. 1] and which includes:

- **Stakeholder Interest Identification:** Identify the primary (e.g., CISO, CIO, CTO) and secondary C-SCRM stakeholders (e.g., CEO/Head of Agency, COO, CFO), and define/measure requirements based on the context required for each stakeholder or stakeholder group.
- **Goals and Objectives Definition:** Identify and document enterprise strategic and C-SCRM-specific performance goals and objectives. These goals may be expressed in the form of enterprise strategic plans, C-SCRM policies, requirements, laws, regulations, etc.
- **C-SCRM Policies, Guidelines, and Procedure Review:** Identify the desired C-SCRM practices, controls, and expectations outlined within these documents and used to guide/implement C-SCRM across the enterprise.
- **C-SCRM Program Implementation Review:** Collect any existing data, measures, and evidence that can provide insights used to derive new measures. These may be found in C-SCRM Plans, POA&Ms, supplier assessments, etc.
- **Level of Implementation:** Develop and map measures to the identified C-SCRM standards, policies, and procedures to demonstrate the program's implementation

progress. These measures should be considered when rendering decisions to prioritize and invest in C-SCRM capabilities.

- **C-SCRM Program Results on Efficiency and Effectiveness:** Develop and map measures of C-SCRM's efficiency and effectiveness to the identified strategy and policy objectives to gauge whether desired C-SCRM outcomes are met. These measures should be considered part of policy refreshes.
- **Business and Mission Impact:** Develop and map measures to the identified enterprise strategic and C-SCRM-specific objectives to offer insight into the impact of C-SCRM (e.g., contribution to business process cost savings; reduction in national security risk). These measures should be considered a component of goal and objective refreshes.

Similar to information security measures, C-SCRM-focused measures can be attained at different levels of an enterprise. Table 3-4 provides example measurement topics across the three Risk Management levels.

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

Risk Management Level	Example Measurement Topics
Level 1	• Policy adoption at lower levels • Timeliness of policy adoption at lower levels • Adherence to risk appetite and tolerance statements • 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 and business process-level risk exposure • Degree and quality of C-SCRM requirement adoption in mission and business processes • Use of a C-SCRM PMO by Level 3
Level 3	• Design effectiveness of controls • Operating effectiveness of controls • Cost efficiency of controls

Enterprises should validate identified C-SCRM goals and objectives with their targeted stakeholder groups prior to beginning an effort to develop specific measures. When developing C-SCRM measures, enterprises should focus on the stakeholder's highest priorities and target measures based on data that can be realistically sourced and gathered. Each established measure should have a specified performance target used to gauge whether goals and objectives in relation to that measure are being met. Enterprises should consider the use of measures templates to formalize each measure and serve as a source of reference for all information pertaining to that measure. Finally, enterprises should develop a formal feedback loop with stakeholders to ensure

that measures are continually providing the desired insights and remain aligned with the enterprise's overall strategic objectives for C-SCRM.

3.6. Dedicated Resources

To appropriately manage cybersecurity risks throughout the supply chain, enterprises should dedicate funds toward this effort. Identifying resource needs and taking steps to secure adequate, recurring, and dedicated funding are essential and important activities that need to be built into the C-SCRM strategy and implementation planning effort and incorporated into an enterprise's budgeting, investment review, and funds management processes. Access to adequate resources is a critical, key enabler for the establishment and sustainment of a C-SCRM program capability. Where feasible, enterprises should be encouraged to leverage existing fund sources to improve their C-SCRM posture. The continued availability of dedicated funds will allow enterprises to sustain, expand, and mature their capabilities over time.

Securing and assigning C-SCRM funding is representative of leadership's commitment to the importance of C-SCRM, 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 enterprises begin by defining a set of goals and objectives upon which to build a strategic roadmap, laying out the path to achieving them through the assignment and allocation of finite resources. The establishment of dedicated funding tied to C-SCRM objectives sets conditions for accountability of performance and compels responsible staff to be efficient, effective, and 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 accomplished 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 enterprise's mission and 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 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, acquire contractor support to aid in developing C-SCRM program guidance, or 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 toward C-SCRM efforts or new or additional funds requested. Enterprises should also seek out opportunities to leverage shared services whenever practical.

The use of shared services can optimize the use of scarce resources and concentrate capability into centers of excellence that provide cost-efficient access to services, systems, or tools. Enterprises can adopt cost-sharing mechanisms across their lower-level entities that allow cost-efficient access to C-SCRM resources and capabilities. Enterprises that pursue shared-services models for C-SCRM should also be aware of the challenges of such models. Shared services (e.g., C-SCRM PMO) are most effective when the enterprise at large relies on a fairly homogenous set of C-SCRM strategies, policies, and processes. In many instances, the centralized delivery of C-SCRM services requires a robust technology infrastructure. The enterprise'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/finance officials is critical to understanding what options may be available and viable in the near term and out-years. These officials can also advise on how best to justify needs, as well as the timeframes and processes for requesting new funds. There are likely different processes to follow for securing recurring funds versus 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 presented to an enterprise's investment review board for approval. Organizations may find it helpful to break out resource needs into ongoing and one-time costs or into cost categories that align with budget formulation, resource decision-making, and the allocation and management of available funds.

It is recommended that the C-SCRM PMO have the lead responsibility of coordinating with mission and 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 the amount of funding required, when, and for what purpose, enterprises 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 cost 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, tools, or systems. This will provide the enterprise with 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 dispersed across the enterprise and reflected in individual office or mission and business process-area budgets. Regardless of how funds are actually assigned, a centralized picture of the C-SCRM budget and funds status will provide a valuable source of information that justifies new requests, informs prioritization decisions, and adjusts expectations about certain activities and the duration in which they can be accomplished.

Ensuring that C-SCRM program funding is distinctly articulated within the enterprise's budget – with performance measures linked to the funding – will drive accountability for results. The visible dedication of funds in budget requests, performance plans, and reports compels leadership attention on C-SCRM processes and the accomplishment of objectives. Budgets must be requested and justified on a periodic basis. 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.

Key Takeaways[34]

C-SCRM in Acquisition. Th eintegration of C-SCRM into acquisition activities is critical to the success of any C-SCRM program. C-SCRM requirements should be embedded throughout the acquisition life cycle. The C-SCRM activities include performing risk assessments of services, suppliers, and products; identifying relevant C-SCRM controls; conducting due diligence; and continuously monitoring suppliers.

Supply Chain Information Sharing. Enterprises will gain access to information critical to understanding and mitigating cybersecurity risks throughout the supply chain by building information-sharing processes and activities into C-SCRM programs. Enterprises should engage with peers, business partners, suppliers, and information-sharing communities (e.g., ISACs) to gain insight into cybersecurity risks throughout the supply chain and learn from the experiences of the community at large.

C-SCRM Awareness and Training. Enterprises should adopt enterprise-wide and role-based training programs to educate users on the potential impact that cybersecurity risks throughout the supply chain can have on the business and how to adopt best practices for risk mitigation. Robust C-SCRM training is a key enabler for enterprises as they shift toward a C-SCRM-aware culture.

C-SCRM Key Practices. This publication outlines several Foundational, Sustaining, and Enabling C-SCRM practices that enterprises should adopt and tailor to their unique contexts. Enterprises should prioritize reaching a base level of maturity in key practices before focusing on advanced C-SCRM capabilities.

Capability Implementation Measurement and C-SCRM Measures. Enterprises should actively manage the efficiency and effectiveness of their C-SCRM programs. First, enterprises should adopt a C-SCRM framework as the basis for measuring their progress toward C-SCRM objectives. Next, enterprises should create and implement quantitative performance measures and target tolerance that provide a periodic glimpse into the enterprise's progress through the lens of specific operational objectives.

Dedicated Resources. Where possible and applicable, enterprises should commit dedicated funds to C-SCRM. The benefits of doing so include facilitating strategic and goal-oriented planning, driving accountability of internal stakeholders to execute and mature the C-SCRM practices of the enterprise, and the continuous monitoring of progress by enterprise leadership.

[34] Key takeaways describe key points from the section text. Refer to the Glossary in Appendix H for definitions.

REFERENCES

[CISA SCRM WG3] Cybersecurity and Infrastructure Agency – Working Group 3 (2021) *Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists* (Arlington, Virginia). Available at https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Qualified-Bidders-Lists_508.pdf

[COSO 2011] Rittenberg L, Martens F (2012) *Enterprise Risk Management: Understanding and Communicating Risk Appetite.* (Committee of Sponsoring Organizations of the Treadway Commission), Thought Leadership in ERM. Available at https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf

[COSO 2020] Martens F, Rittenberg L (2020) *Risk Appetite – Critical to Success: Using Risk Appetite To Thrive in a Changing World*. (Committee of Sponsoring Organization of the Treadway Commission), Thought Leadership in ERM. Available at https://www.coso.org/Documents/COSO-Guidance-Risk-Appetite-Critical-to-Success.pdf

[Defense Industrial Base Assessment: Counterfeit Electronics] Bureau of Industry and Security, Office of Technology Evaluation (2010) *Defense Industrial Base Assessment: Counterfeit Electronics*. (U.S. Department of Commerce, Washington, D.C.). Available at https://www.bis.doc.gov/index.php/documents/technology-evaluation/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010/file

[FedRAMP] General Services Administration (2022) *FedRAMP*. Available at http://www.fedramp.gov/

[GAO] Government Accountability Office (2020) *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*. (U.S. Government Accountability Office, Washington D.C.), Report to Congressional Requesters GAO-21-171. Available at https://www.gao.gov/assets/gao-21-171.pdf

[CNSSI 4009] Committee on National Security Systems (2015) *Committee on National Security Systems (CNSS) Glossary* (CNSS, Ft. Meade, Md.), CNSSI 4009-2015. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[EO 14028] Executive Order 14028 (2021) Improving the Nation's Cybersecurity. (The White House, Washington, DC), DCPD-202100401, May 12, 2021. https://www.govinfo.gov/app/details/DCPD-202100401

[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*, Pub. L. 115-390, 132 Stat. 5173. Available at https://www.congress.gov/115/plaws/publ390/PLAW-115publ390.pdf

[FIPS 199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[FIPS 200] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200

[FSP] Cyber Risk Institute (2020) *Financial Services Cybersecurity Framework Profile Version 1.0.* Available at https://cyberriskinstitute.org/the-profile/

[ISO 9000] International Organization for Standardization (2015) *ISO 9000:2015 — Quality management — Fundamentals and vocabulary* (ISO, Geneva). Available at https://www.iso.org/standard/45481.html

[ISO 28001] International Organization for Standardization (2007) *ISO 28001:2007 — Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance* (ISO, Geneva). Available at https://www.iso.org/standard/45654.html.

[ISO Guide 73] International Organization for Standardization (2009) *ISO Guide 73:2009 — Risk management — Vocabulary* (ISO, Geneva). Available at https://www.iso.org/standard/44651.html

[ISO/IEC 2382] International Organization for Standardization/International Electrotechnical Commission (2015) *ISO/IEC 2382:2015 — Information technology — Vocabulary* (ISO, Geneva). Available at https://www.iso.org/standard/63598.html

[ISO/IEC 20243] International Organization for Standardization/International Electrotechnical Commission (2018) *ISO/IEC 20243-1:2018 – Information technology — Open Trusted Technology Provider™ Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products Part 1: Requirements and recommendations* (ISO, Geneva). Available at https://www.iso.org/standard/74399.html

[ISO/IEC 27000] International Organization for Standardization/International Electrotechnical Commission (2018) *ISO/IEC 27000:2018 – Information technology – Security techniques – Information security management systems – Overview and vocabulary* (ISO, Geneva). Available at https://www.iso.org/standard/73906.html

[ISO/IEC 27002] International Organization for Standardization/International Electrotechnical Commission (2022) *ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information security controls* (ISO, Geneva). Available at https://www.iso.org/standard/75652.html

[ISO/IEC 27036] International Organization for Standardization/International Electrotechnical Commission (2014) *ISO/IEC 27036-2:2014 – Information technology – Security techniques – Information security for supplier relationships – Part 2: Requirements* (ISO, Geneva). Available at https://www.iso.org/standard/59680.html

[ISO/IEC/IEEE 15288] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2015) *ISO/IEC/IEEE 15288:2015 — Systems and software engineering — System life cycle processes* (ISO, Geneva). Available at https://www.iso.org/standard/63711.html

[ITIL Service Strategy] Cannon D (2011) *ITIL Service Strategy* (The Stationary Office, London), 2nd Ed.

[NDIA] National Defense Industrial Association System Assurance Committee (2008) *Engineering for System Assurance*. (NDIA, Arlington, VA). Available at https://www.ndia.org/-/media/sites/ndia/meetings-and-events/divisions/systems-engineering/sse-committee/systems-assurance-guidebook.ashx.

[NIST CSF] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[NIST SCRM Proceedings 2012] National Institute of Standards and Technology (2012) *Summary of the Workshop on Information and Communication Technologies Supply Chain Risk Management*. Available at https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=913338

[NIST SP 800-16] deZafra DE, Pitcher SI, Tressler JD, Ippolito JB (1998) Information Technology Security Training Requirements: a Role- and Performance-Based Model. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-16. https://doi.org/10.6028/NIST.SP.800-16

[NIST SP 800-30 Rev. 1] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[NIST SP 800-32] Kuhn DR, Hu VC, Polk WT, Chang S-jH (2001) Introduction to Public Key Technology and the Federal PKI Infrastructure. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-32. https://doi.org/10.6028/NIST.SP.800-32

[NIST SP 800-34 Rev. 1] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34,

Rev. 1, Includes updates as of November 11, 2010. https://doi.org/10.6028/NIST.SP.800-34r1

[NIST SP 800-37] Joint Task Force (2018) 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), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[NIST SP 800-39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[NIST SP 800-53 Rev. 5] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[NIST SP 800-53A Rev. 5] Joint Task Force (2022) Assessing Security and Privacy Controls in Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53Ar5

[NIST SP 800-53B] Joint Task Force (2020) Control Baselines for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53B

[NIST SP 800-55 Rev. 1] Chew E, Swanson MA, Stine KM, Bartol N, Brown A, Robinson W (2008) Performance Measurement Guide for Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-55, Rev. 1. https://doi.org/10.6028/NIST.SP.800-55r1

[NIST SP 800-64] Kissel R, Stine KM, Scholl MA, Rossman H, Fahlsing J, Gulick, J (2008) Security Considerations in the System Development Life Cycle. (National Institute of Standards and Technology, Gaithersburg, MD), (Withdrawn) NIST Special Publication (SP) 800-64 Rev. 2. https://doi.org/10.6028/NIST.SP.800-64r2

[NIST SP 800-100] Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007. https://doi.org/10.6028/NIST.SP.800-100

[NIST SP 800-115] Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical Guide to Information Security Testing and Assessment. (National Institute of Standards

and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-115. https://doi.org/10.6028/NIST.SP.800-115

[NIST SP 800-160 Vol. 1] Ross RS, Oren JC, McEvilley M (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. https://doi.org/10.6028/NIST.SP.800-160v1

[NIST SP 800-160 Vol. 2] Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2021) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-160v2r1

[NIST SP 800-171 Rev. 2] Ross RS, Pillitteri VY, Dempsey KL, Riddle M, Guissanie G (2020) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171, Rev. 2, Includes updates as of January 28, 2021. https://doi.org/10.6028/NIST.SP.800-171r2

[NIST SP 800-172] Ross RS, Pillitteri VY, Guissanie G, Wagner R, Graubart R, Bodeau D (2021) Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-172. https://doi.org/10.6028/NIST.SP.800-172

[NIST SP 800-181 Rev. 1] Petersen R, Santos D, Wetzel KA, Smith MC, Witte GA (2017) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1

[NIST SSDF] National Institute of Standards and Technology (2022) *NIST Secure Software Development Framework*. Available at https://csrc.nist.gov/projects/ssdf

[NISTIR 7622] Boyens JM, Paulsen C, Bartol N, Shankles S, Moorthy R (2012) Notional Supply Chain Risk Management Practices for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7622. https://doi.org/10.6028/NIST.IR.7622

[NISTIR 8179] Paulsen C, Boyens JM, Bartol N, Winkler K (2018) Criticality Analysis Process Model: Prioritizing Systems and Components. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8179. https://doi.org/10.6028/NIST.IR.8179

[NISTIR 8276] Boyens J, Paulsen C, Bartol N, Winkler K, Gimbi J (2021) Key Practices in Cyber Supply Chain Risk Management: Observations from Industry. (National Institute of

Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8276. https://doi.org/10.6028/NIST.IR.8276

[NISTIR 8286] Stine KM, Quinn SD, Witte GA, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286

[NTIA SBOM] *The Minimum Elements For a Software Bill of Materials (SBOM)*, NTIA and Department of Commerce, 2021 https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

[OMB A-123] Office of Management and Budget (2004) Management's Responsibility for Internal Control. (The White House, Washington, DC), OMB Circular A-123, December 21, 2004. Available at https://georgewbush-whitehouse.archives.gov/omb/circulars/a123/a123_rev.html

[OMB A-130] Office of Management and Budget (2016) Managing Information as a Strategic Resource. (The White House, Washington, DC), OMB Circular A-130, July 28, 2016. Available at https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

[SAFECode 1] Software Assurance Forum for Excellence in Code (2010) *Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain*. Available at http://www.safecode.org/publications/SAFECode_Software_Integrity_Controls0610.pdf

[SAFECode 2] Software Assurance Forum for Excellence in Code (2009) *The Software Supply Chain Integrity Framework: Defining Risks and Responsibilities for Securing Software in the Global Supply Chain*. Available at http://www.safecode.org/publication/SAFECode_Supply_Chain0709.pdf

[SwA] Polydys ML, Wisseman S (2008) *Software Assurance in Acquisition: Mitigating Risks to the Enterprise. A Reference Guide for Security-Enhanced Software Acquisition and Outsourcing.* (National Defense University Press, Washington, D.C.) Information Resources Management College Occasional Paper. Available at https://apps.dtic.mil/dtic/tr/fulltext/u2/a495389.pdf

APPENDIX A: C-SCRM SECURITY CONTROLS [35]

C-SCRM CONTROLS INTRODUCTION

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 199]

[NIST SP 800-53, Rev. 5] defines numerous cybersecurity 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 20 control families of [NIST SP 800-53, Rev. 5]. This approach facilitates use of the security controls assessment techniques articulated in [NIST SP 800-53A, Rev. 5] to assess implementation of C-SCRM controls.

The controls provided in this publication are intended for enterprises to implement internally and to require of their contractors and subcontractors if and when applicable and as articulated in 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 enterprise'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.

C-SCRM CONTROLS SUMMARY

During the Respond step of the risk management process articulated in Section 2, enterprises select, tailor, and implement controls for mitigating cybersecurity risks throughout the supply chain. [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 supply chain infrastructure. The section provides 20 C-SCRM control families that include relevant controls and supplemental guidance.

Figure A-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 and represents the following steps:

1. Select and extract individual controls and enhancements from [NIST SP 800-53, Rev. 5] applicable to C-SCRM.
2. Analyze these controls to determine how they apply to C-SCRM.

[35] Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

3. Evaluate the resulting set of controls and enhancements to determine whether all C-SCRM concerns were addressed.
4. Develop additional controls currently undefined in [NIST SP 800-53, Rev. 5].
5. Identify controls for flow down to relevant sub-level contractors.
6. Assign applicable levels to each C-SCRM control.
7. Develop C-SCRM-specific supplemental guidance for each C-SCRM control.

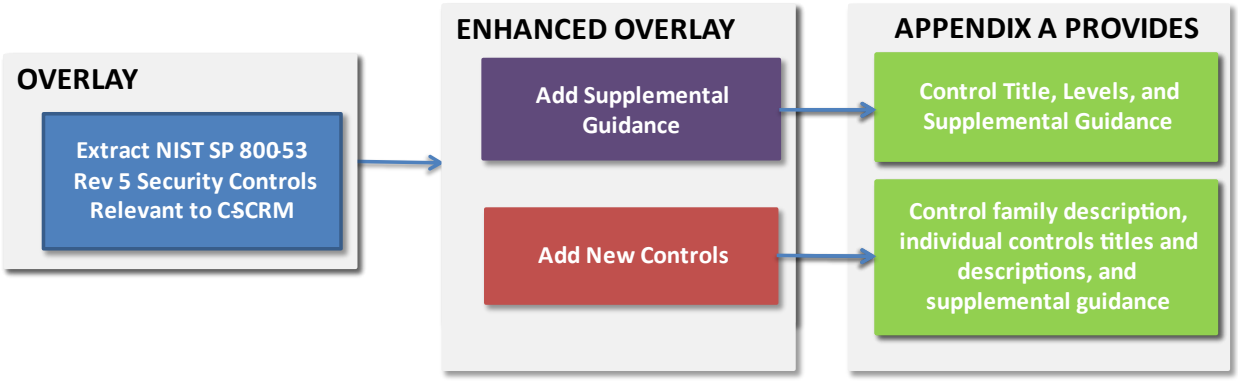

Fig. A-1: C-SCRM Security Controls in NIST SP 800-161, Rev. 1

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.

C-SCRM CONTROLS THROUGHOUT THE ENTERPRISE

As noted in Table A-1, C-SCRM controls in this publication are designated by the three levels comprising the enterprise. This is to facilitate the selection of C-SCRM controls specific to enterprises, their various missions, and individual systems, as described in Appendix C under the Respond step of the risk management process. During controls selection, enterprises 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, enterprises will ensure that they have appropriately addressed C-SCRM.

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 enterprises 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 throughout their acquisition activities. More detail on the role of C-SCRM in acquisition is provided in Section 3.1 of this document.

It is important to recognize that the controls in this section do not provide specific contracting language. Acquirers should use this publication as guidance to develop their own contracting language with specific C-SCRM requirements for inclusion. The following sections expand upon the supplier, developer, system integrator, external system service provider, and other ICT/OT-related service provider roles with respect to C-SCRM expectations for acquirers.

Enterprises may use multiple techniques to ascertain whether these controls are in place, such as supplier self-assessment, acquirer review, or third-party assessments for measurement and adherence to the enterprise's requirements. Enterprises should first look to established third-party assessments to see if they meet their needs. When an enterprise defines C-SCRM requirements, it may discover that established third-party assessments may not address all specific requirements. In this case, additional evidence may be needed to justify unaddressed requirements. Please note that the data obtained for this purpose should be appropriately protected.

SUPPLIERS

Suppliers may provide either commercial off-the-shelf (COTS) or, in federal contexts, government off-the-shelf (GOTS) solutions to the acquirer. COTS solutions include non-developmental items (NDI), such as commercially-licensed solutions/products. GOTS solutions are government-only licensable solutions. Suppliers are a diverse group that ranges from very small to large, specialized to diversified, and based in a single country to transnational. Suppliers also range widely in their level of sophistication, resources, and transparency/visibility into their processes and solutions.

Suppliers have diverse levels and types of C-SCRM practices in place. These practices and other related practices may provide the requisite evidence for SCRM evaluation. An example of a federal resource that may be leveraged is the Defense Microelectronics Activity (DMEA) accreditation for trusted suppliers. When appropriate, allow suppliers the opportunity to reuse any existing data and documentation that may provide evidence of C-SCRM implementation.

Enterprises should consider whether the cost of doing business with suppliers may be directly impacted by the extent of supply chain cybersecurity requirements imposed on suppliers, the willingness or ability of suppliers to allow visibility into how their products are developed or manufactured, and how they apply security and supply chain practices to their solutions. When enterprises or system integrators require greater levels of transparency from suppliers, they must consider the possible cost implications of such requirements. Suppliers may opt not to participate in procurements to avoid increased costs or perceived risks to their intellectual property, limiting an enterprise's supply or technology choices. Additionally, suppliers may face risks from customers imposing multiple and different sets of supply chain cybersecurity requirements with which the supplier must comply on a per-customer basis. The amount of transparency required from suppliers should be commensurate to the suppliers' criticality, which is sufficient to address inherent risk.

DEVELOPERS AND MANUFACTURERS

Developers and manufactures 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 enterprises 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.

SYSTEM INTEGRATORS

System integrators 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 solution or service that is customized to the acquirer's requirements. Such proposals provided by system integrators can include many layers of suppliers and teaming arrangements with other vendors or subcontractors. The system integrator should ensure that 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 and any relevant countermeasures to address identified or potential risks.

EXTERNAL SYSTEM SERVICE PROVIDERS OF INFORMATION SYSTEM SERVICES

Enterprises 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 cybersecurity supply chain concerns that reduces the acquirer's visibility into and control of the outsourced functions. Therefore, it requires increased rigor from enterprises in defining C-SCRM requirements, stating them in procurement agreements, 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 enterprise's systems and data that result from the use of these services. Enterprises should implement a set of compensating C-SCRM controls to address this risk and work with the mission and 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.

OTHER ICT/OT-RELATED SERVICE PROVIDERS

Providers of services can perform a wide range of different functions, ranging from consulting to publishing website content to janitorial services. Other ICT/OT-related service providers encompass those providers that require physical or logical access to ICT/OT or the 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 of delivering their service. As a result of service provider access or use, the potential for cyber supply chain risk being introduced to the enterprise rises.

Operational technology possesses unique operational and security characteristics that necessitate the application of specialized skills and capabilities to effectively protect them. Enterprises that have significant OT components throughout their enterprise architecture often turn to specialized

service providers for the secure implementation and maintenance of these devices, systems, or equipment. Any enterprise or individual providing services that may include authorized access to an ICT or OT system should adhere to enterprise C-SCRM requirements. Enterprises should apply special scrutiny to ICT/OT-related service providers managing mission-critical and/or safety-relevant assets.

SELECTING, TAILORING, AND IMPLEMENTING C-SCRM SECURITY CONTROLS

The C-SCRM controls defined in this section should be selected and tailored according to individual enterprise needs and environments using the guidance in [NIST SP 800-53, Rev. 5] in order to ensure a cost-effective, risk-based approach to providing enterprise-wide C-SCRM. The C-SCRM baseline defined in this publication addresses the basic needs of a broad and diverse set of constituents. Enterprises must select, tailor, and implement the security controls based on: (i) the environments in which enterprise information systems are acquired and operate; (ii) the nature of operations conducted by enterprises; (iii) the types of threats facing enterprises, mission and 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 enterprise. The tailoring should be coordinated with and approved by the appropriate enterprise 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, enterprises 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 enterprise officials as part of the C-SCRM plan approval process.

C-SCRM CONTROL FORMAT

Table A-1 shows the format used in this publication for controls providing 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 A-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. Enterprises 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 enterprise's system. For example, in a "badge flipping" situation, a contract is transferred from one system integrator enterprise to another with the same personnel supporting the contract. In that situation, the enterprise should disable the existing accounts, retire the old credentials, establish new accounts, and issue completely new credentials.

Level(s): 2, 3

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, Rev. 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, then the parent control number and title are included, but there is no supplemental C-SCRM guidance.
- C-SCRM controls/enhancements that do not have an associated [NIST SP 800-53, Rev. 5] control/enhancement are listed with their titles and the control/enhancement text.
- All C-SCRM controls include the levels for 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
- The C-SCRM Control SR-13 – Supplier Inventory is added to the Supply Chain Risk Management control family

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, devices (including other information systems), and 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 enterprises, 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 the unauthorized release, modification, or destruction of information. This access should be limited to only the necessary type, duration, and level of access for authorized enterprises (and authorized individuals within those enterprises) and monitored for cybersecurity supply chain impact.

AC-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: Enterprises 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 that have access control policies. These should include both physical and logical access to the supply chain and the information system. Enterprises should require their 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 supply chain. This control also helps ensure access authorizations of actors in the supply chain is appropriate on a continuous basis. The enterprise may choose to define a set of roles and associate a level of authorization to ensure proper implementation. Enterprises 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. Enterprises 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. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

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. Enterprises should ensure that a defined consequence framework is in place to address access control violations. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with *Executive Order 14028, Improving the Nation's Cybersecurity*.

Level(s): 2, 3

Control Enhancement(s):

(1) *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 enterprise's system. Enterprises 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 enterprise. Enterprises must also 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 enterprise to another with the same personnel supporting the contract. In that situation, the enterprise should disable the existing accounts, retire the old credentials, establish new accounts, and issue completely new credentials.

Level(s): 2, 3

(2) *ACCESS ENFORCEMENT | CONTROLLED RELEASE*

Supplemental C-SCRM Guidance: Information about the supply chain should be controlled for release between the enterprise and third parties. Information may be exchanged between the enterprise and its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The controlled release of enterprise information protects against risks associated with disclosure.

Level(s): 2, 3

AC-4 INFORMATION FLOW ENFORCEMENT

Supplemental C- SCRM Guidance: Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Specifying the requirements and how information flow is enforced should ensure that only the required information is communicated to various participants in the supply chain. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

Control Enhancement(s):

(1) *INFORMATION FLOW ENFORCEMENT | METADATA*

Supplemental C-SCRM Guidance: The metadata relevant to C-SCRM is 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. Enterprises 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

(2) *INFORMATION FLOW ENFORCEMENT | DOMAIN AUTHENTICATION*

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

Level(s): 2, 3

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

Supplemental C-SCRM Guidance: For C-SCRM, the validation of data and the relationship to its metadata are critical. Much of the data transmitted through the 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 supply chain.

Level(s): 2, 3

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

Supplemental C-SCRM Guidance: The enterprise should ensure the separation of the information system and supply chain information[36] flow. Various mechanisms can be implemented, such as encryption methods (e.g., digital signing). Addressing information flow between the enterprise 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 enterprise should ensure that an appropriate separation of duties is established for decisions that require the acquisition of both information system and supply chain components. The separation of duties helps to ensure that adequate protections are in place for components entering the enterprise's supply chain, such as denying developers the privilege to promote code that they wrote from development to production environments. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

[36] Supply Chain Cybersecurity Risk Information is defined in the glossary of this document based on the Federal Acquisition Supply Chain Security Act (FASCSA) definition for the term.

Level(s): 2, 3

AC-6 LEAST PRIVILEGE

Supplemental C-SCRM Guidance: For C-SCRM supplemental guidance, see control enhancements. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Control Enhancement(s):

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

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

Level(s): 2, 3

AC-17 REMOTE ACCESS

Supplemental C-SCRM Guidance: Ever more frequently, supply chains are accessed remotely. Whether for the purpose of development, maintenance, or the operation of information systems, enterprises should implement secure remote access mechanisms and allow remote access only to vetted personnel. Remote access to an enterprise's supply chain (including distributed software development environments) should be limited to the enterprise or contractor personnel and only if and as required to perform their tasks. Remote access requirements – such using a secure VPN, employing multi-factor authentication, or limiting access to specified business hours or from specified geographic locations – must be properly defined in agreements. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

Control Enhancement(s):

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

Supplemental C-SCRM Guidance: Enterprises should ensure that detailed requirements are properly defined and that access to information regarding the information system and supply chain is protected from unauthorized use and disclosure. Since supply chain data and metadata disclosure or access can have significant implications for an enterprise's mission processes, appropriate measures must be taken to vet both the 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 enterprise's 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 supply chain as they are moved from one location to another, whether within the enterprise's own environment or during delivery from system integrators or suppliers. Ensuring that appropriate and secure access mechanisms are in place within this 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 enterprise should explicitly define appropriate wireless access control mechanisms for the supply chain in policy and implement appropriate mechanisms.

Level(s): 1, 2, 3

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Supplemental C-SCRM Guidance: The use of mobile devices (e.g., laptops, tablets, e-readers, smartphones, smartwatches) has become common in the supply chain. They are used in direct support of an enterprise's operations, as well as tracking, supply chain logistics, data as information systems, and components that traverse enterprise or systems integrator supply chains. Ensure that access control mechanisms are clearly defined and implemented where relevant when managing enterprise 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: Enterprises' 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 enterprise 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 supply chain from such external information systems should be monitored and audited. Enterprises should require their 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 supply chain to the systems of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

Level(s): 2, 3

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

Supplemental C-SCRM Guidance: Devices that do not belong to the enterprise (e.g., bring your own device [BYOD] policies) increase the enterprise's exposure to cybersecurity risks throughout the supply chain. This includes devices used by suppliers, developers, system integrators, external system

service providers, and other ICT/OT-related service providers. Enterprises should review the use of non-enterprise devices by non-enterprise personnel and make a risk-based decision as to whether it will allow the use of such devices or furnish devices. Enterprises should furnish devices to those non-enterprise personnel who present unacceptable levels of risk.

Level(s): 2, 3

AC-21 INFORMATION SHARING

Supplemental C-SCRM Guidance: Sharing information within the supply chain can help manage cybersecurity risks throughout the supply chain. This information may include vulnerabilities, threats, the criticality of systems and components, or delivery information. This information sharing should be carefully managed to ensure that the information is only accessible to authorized individuals within the enterprise's supply chain. Enterprises should clearly define boundaries for information sharing with respect to temporal, informational, contractual, security, access, system, and other requirements. Enterprises should monitor and review for unintentional or intentional information sharing within its 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, whether alone or with other information.

Level(s): 2, 3

AC-23 DATA MINING PROTECTION

Supplemental C-SCRM Guidance: Enterprises should require their 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: Enterprises should assign access control decisions to support authorized access to the 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. This may require defining such requirements in service-level agreements, in many cases as part of the upfront relationship established between the enterprise and system integrator or the enterprise and external service provider. Enterprises should require their 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.

This document 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 the appropriate processes and controls that can help mitigate cybersecurity risks throughout the supply chain. Enterprises should provide C-SCRM awareness and training to individuals at all levels within the enterprise, including information security, procurement, enterprise risk management, engineering, software development, IT, legal, HR, and others. Enterprises should also work with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to ensure that the personnel who interact with an enterprise's supply chains receive C-SCRM awareness and training, as appropriate.

AT-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: Enterprises should designate a specific official to manage the development, documentation, and dissemination of the training policy and procedures, including C-SCRM and role-based specific training for those with supply chain responsibilities. Enterprises should integrate cybersecurity supply chain risk management training and awareness into the security training and awareness policy. C-SCRM training should target both the enterprise and its contractors. The policy should ensure that supply chain cybersecurity role-based training is required for those individuals or functions that touch or impact the supply chain, such as the 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 supply chain and system/element life cycle to limit the opportunities and means available to individuals performing these roles that could result in adverse consequences,
b. Requirements for interaction between an enterprise's personnel and individuals not employed by the enterprise who participate in the 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 is provided in the control enhancements. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Control Enhancements:

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

Supplemental C-SCRM Guidance: Enterprises should provide practical exercises in literacy training that simulate supply chain cybersecurity events and incidents. Enterprises should require their 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: Enterprises should provide literacy training on recognizing and reporting potential indicators of insider threat within the supply chain. Enterprises should require their 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: Enterprises should provide literacy training on recognizing and reporting potential and actual instances of supply chain-related social engineering and social mining. Enterprises should require their 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 or anomalous behavior in enterprise supply chain systems. Enterprises should require their 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 an advanced persistent threat (APT) in the enterprise's supply chain. Enterprises should require their 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 enterprise's supply chain environment. Enterprises should require their 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 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. Responding to threats and identified risks requires training in counterintelligence awareness and reporting. Enterprises should ensure that developers receive training on secure development practices as well as the use of vulnerability scanning tools. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should

refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

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, receiving, physical access to facilities, inventory management, and warehousing. Enterprise and system integrator personnel who provide development and operational support to the enterprise should receive training on how to handle these physical security mechanisms and on the associated cybersecurity risks throughout the supply chain.

Level(s): 2

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

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

Level(s): 2

AT-4 TRAINING RECORDS

Supplemental C-SCRM Guidance: Enterprises should maintain documentation for C-SCRM-specific training, especially with 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 that is useful in the event of a supply chain cybersecurity incident or compromise. Enterprises should ensure that they designate and audit cybersecurity 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 a reasonable time frame, as defined by enterprise policy. Enterprises 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 requirements for such monitoring in agreements. However, enterprises should not deploy audit mechanisms on systems outside of their enterprise 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: Enterprises 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. The audit and accountability policy and procedures should appropriately address tracking activities and their 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 a policy unless those functions 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 they present to the enterprise and the enterprise'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 enterprise's SDLC context and requirements. Auditable events may include software/hardware changes, failed attempts to access supply chain information systems, or the movement of source code. Information on such events should be captured by appropriate audit mechanisms and be traceable and verifiable. Information captured may include the type of event, date/time, length, and the frequency of occurrence. Among other things, auditing may help detect misuse of the supply chain information systems or network caused by insider threats. Logs are a key resource when identifying operational trends and long-term problems. As such, enterprises should incorporate reviewing logs at the contract renewal point for vendors to determine whether there is a systemic problem. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should

refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 1, 2, 3

AU-3 CONTENT OF AUDIT RECORDS

Supplemental C-SCRM Guidance: The audit records of a supply chain event should be securely handled and maintained in a manner that conforms to record retention requirements and preserves the integrity of the findings and the confidentiality of the record information and its sources as appropriate. In certain instances, such records may be used in administrative or legal proceedings. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 1, 2, 3

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

Supplemental C-SCRM Guidance: The enterprise 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 an invalid signature is an information security auditable event. The combination of these two events may provide information valuable to C-SCRM. The enterprise should adjust the level of audit record review based on the 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):

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

Supplemental C-SCRM Guidance: In a C-SCRM context, non-technical sources include changes to the enterprise's security or operational policy, changes to the 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: Enterprises should implement non-repudiation techniques to protect the originality and integrity of both information systems and the supply chain network. Examples of what may require non-repudiation include supply chain metadata that describes the components, supply chain communication, and delivery acceptance information. For information systems, examples may include patch or maintenance upgrades for software as well as component replacements 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 the supply chain and 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 supply chain. It also helps the verification of system and component integrity.

Level(s): 2, 3

AU-12 AUDIT RECORD GENERATION

Supplemental C-SCRM Guidance: Enterprises 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. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

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 enterprise's system that increases the risk to that system. Enterprises should ensure that monitoring is in place for contractor systems to detect the unauthorized disclosure of any data and that contract language includes a requirement that the vendor will notify the enterprise, in accordance with enterprise-defined time frames and as soon as possible in the event of any potential or actual unauthorized disclosure. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

AU-14 SESSION AUDIT

Supplemental C-SCRM Guidance: Enterprises should include non-federal contract employees in session audits to identify security risks in the supply chain. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and

agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

AU-16 CROSS-ORGANIZATIONAL AUDIT LOGGING

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

Level(s): 2, 3

Control Enhancement(s):

(4) *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 enterprises and its system integrators or external services providers, enterprises 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 enterprise, a service-level agreement of the type of audit data required versus what can be provided must be agreed to in advance to ensure that the enterprise obtains the relevant audit information needed to ensure that appropriate protections are in place to meet its mission operation protection needs. Ensure that coverage of both the information systems and supply chain network are addressed for the collection and sharing of audit information. Enterprises should require their 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.

Enterprises 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 enterprise'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. Supply chain aspects include documentation, the tracking of chain of custody and system interconnections within and between enterprises, the verification of supply chain cybersecurity training, the verification of suppliers' claims of conformance to security, product/component integrity, and validation tools and techniques for non-invasive 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 supply chain cybersecurity into the control assessment and authorization policy and related C-SCRM Strategy/Implementation Plan(s), policies, and system-level plans. To address cybersecurity risks throughout the supply chain, enterprises 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 enterprise for conducting control assessment and authorization, any dependencies among those roles, and the interaction among the roles. Enterprise-wide security and privacy risks 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 enterprise-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. Enterprises should develop a strategy for collecting information, including a strategy for engaging with providers on supply chain risk assessments. Such collaboration helps enterprises 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):

(1) *CONTROL ASSESSMENTS | SPECIALIZED ASSESSMENTS*

Supplemental C-SCRM Guidance: Enterprises should use a variety of assessment techniques and methodologies, such as continuous monitoring, insider threat assessment, and malicious user assessment. These assessment mechanisms are context-specific and require the enterprise 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

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

Supplemental C-SCRM Guidance: For C-SCRM, enterprises 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. Certifications from the International Enterprise for Standardization (ISO), the National Information Assurance Partnership (Common Criteria), and the Open Group Trusted Technology Forum (OTTF) may also be used by non-federal and federal enterprises alike, if such certifications meet agency needs.

Level(s): 3

CA-3 INFORMATION EXCHANGE

Supplemental C-SCRM Guidance: The exchange of information or data between the system and other systems requires scrutiny from a supply chain perspective. This includes understanding the interface characteristics and connections of those components/systems that are directly interconnected 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. Proper service-level agreements should be in place to ensure compliance to system information exchange requirements defined by the enterprise, as the transfer of information between systems in different security or privacy domains with different security or privacy policies introduces the 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 enterprise and system integrator
b. Product update/patch management connection to an off-the-shelf supplier
c. Data request and retrieval transactions in a processing system that resides on an external service provider shared environment

Enterprises should require their 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 a system-level plan of actions and milestones (POA&Ms), enterprises need to ensure that a separate POA&M exists for C-SCRM and includes 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, the resources required to accomplish the tasks, milestones established to meet the tasks, and the scheduled completion dates for the milestones and tasks. The enterprise should include relevant weaknesses, the impact of weaknesses on information systems or the supply chain, any remediation to address weaknesses, and any continuous monitoring activities in its C-SCRM POA&M. 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 the C-SCRM POA&M 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 the output of criticality, threat, and vulnerability analyses. Authorizing officials may use the 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. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 1, 2, 3

Control Enhancement(s):

(3) *CONTINUOUS MONITORING | TREND ANALYSES*

Supplemental C-SCRM Guidance: The information gathered during continuous monitoring/trend analyses serves as input into C-SCRM decisions, including criticality analysis, vulnerability and threat analysis, and risk assessments. It also provides information that can be used in incident response and potentially identify a supply chain cybersecurity compromise, including an 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 changes made throughout the SDLC to systems, components, and documentation within the information systems and networks. This is important for knowing what changes were made to those systems, components, and documentation; who made the changes; and who authorized the changes. Configuration management also provides evidence for investigations of supply chain cybersecurity compromise when determining which changes were authorized and which were not. Enterprises should apply configuration management controls to their own systems and encourage the 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 supply chain. Configuration management is critical to the enterprise's ability to establish the provenance of components, including tracking and tracing them through the SDLC and the supply chain. A 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 a configuration management policy and procedures, enterprises should address the full SDLC, including procedures for introducing and removing components to and from the enterprise's information system boundary. A 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 enterprise 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: Enterprises 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 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 enterprise's operational environment and any relevant supplier, developer, system integrator, external system service provider, and other ICT/OT-related service provider involvement with 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.

Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

Control Enhancement(s):

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

Supplemental C-SCRM Guidance: The enterprise 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 staging, if applicable) environments, and any configuration of interfaces.

Level(s): 2, 3

CM-3 CONFIGURATION CHANGE CONTROL

Supplemental C-SCRM Guidance: Enterprises 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. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

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

Supplemental C-SCRM Guidance: Enterprises 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 implementation of the changes.

Level(s): 2, 3

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

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

Level(s): 2, 3

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

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

Level(s): 2, 3

CM-4 IMPACT ANALYSIS

Supplemental C-SCRM Guidance: Enterprises should take changes to the information system and underlying or interoperable systems and networks under consideration to determine whether the impact of these changes affects existing security controls and warrants additional or different protection to maintain an acceptable level of cybersecurity risk throughout the supply chain. 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 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 implementing them into an operational environment, and look 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: Enterprises should ensure that requirements regarding physical and logical access restrictions for changes to the information systems and networks are defined and included in the enterprise'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:

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

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

Level(s): 3

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

Supplemental C-SCRM Guidance: Enterprises 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: Enterprises 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 the creation of the enterprise'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 enterprise personnel when a change has occurred. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

Control Enhancement(s):

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

Supplemental C-SCRM Guidance: The enterprise 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 enterprise should ensure that designated security or IT personnel are alerted to 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 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. Enterprises should select components that allow the flexibility to specify and implement least functionality. Enterprises should ensure least functionality in their information systems and networks and throughout the 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 enterprise systems. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 3

Control Enhancement(s):

(1) *LEAST FUNCTIONALITY | PERIODIC REVIEW*

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

Level(s): 2, 3

(2) *LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE*

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

Level(s): 2, 3

(3) *LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE*

Supplemental C-SCRM Guidance: Enterprises 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 also include requirements for alerts when new software and updates to software are introduced into the enterprise's environment. An example of such requirements is to allow open source software only if the code is available for an enterprise's evaluation and determined to be acceptable for use.

Level(s): 3

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

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

Level(s): 2, 3

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

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

Level(s): 3

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

Supplemental C-SCRM Guidance: When exceptions are made to use software products without accompanying source code and with limited or no warranty because of compelling mission or operational requirements, approval by the authorizing official should be contingent upon the enterprise explicitly incorporating cybersecurity supply chain risk assessments as part of a broader assessment of such software products, as well as the implementation of compensating controls to address any identified and assessed risks.

Level(s): 2, 3

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

Enterprises 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. Enterprises should require their 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: Enterprises should ensure that critical component assets within the information systems and networks are included in the asset inventory. The inventory must also 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 may include the manufacturer, device type, model, serial number, and physical location. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Enterprises should specify the requirements and how information flow is enforced to ensure that only the required information – and no more – is communicated to the various participants in the supply chain. If information is subsetted downstream, there should be information about who created the subset information. Enterprises should consider producing SBOMs for applicable and appropriate classes of software, including purchased software, open source software, and in-house software. Departments and agencies should refer to Appendix F for additional guidance on SBOMs in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

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 enterprise 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 then re-baselined accordingly.

Level(s): 3

(2) *SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE*

Supplemental C-SCRM Guidance: The enterprise 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 enterprise 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

(3) *SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION*

Supplemental C-SCRM Guidance: The enterprise 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

(4) *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 exposure to cybersecurity risks throughout the supply chain.

Level(s): 3

(5) *SYSTEM COMPONENT INVENTORY | CENTRALIZED REPOSITORY*

Supplemental C-SCRM Guidance: Enterprises may choose to implement centralized inventories that include components from all enterprise 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 enterprises rapidly identify the location and responsible individuals of components that have been compromised, breached, or are otherwise in need of mitigation actions. The enterprise should ensure that centralized inventories include the supply chain-specific information required for proper component accountability (e.g., supply chain relevance and information system, network, or component owner).

Level(s): 3

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

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

Level(s): 2, 3

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

Supplemental C-SCRM Guidance: When assigning components to systems, the enterprise 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

(8) *SYSTEM COMPONENT INVENTORY | SBOMs FOR OPEN SOURCE PROJECTS*

Supplemental C-SCRM Guidance: If an enterprise uses an open source project that does not have an SBOM and the enterprise requires one, the enterprise will need to 1) contribute SBOM generation to the open source project, 2) contribute resources to the project to add this capability, or 3) generate an SBOM on their first consumption of each version of the open source project that they use.

Level(s): 3

CM-9 CONFIGURATION MANAGEMENT PLAN

Supplemental C-SCRM Guidance: Enterprises should ensure that C-SCRM is incorporated into configuration management planning activities. Enterprises should require their 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: Enterprises should ensure that all relevant roles are defined to address configuration management activities for information systems and networks. Enterprises should ensure that requirements and capabilities for configuration management are appropriately addressed or included in the following 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: Enterprises 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 the 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 the license documentation should be updated to reflect this change. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

Control Enhancement(s):

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

Supplemental C-SCRM Guidance: When considering software, enterprises should review all options and corresponding risks, including open source or commercially licensed components. When using open source software (OSS), the enterprise should understand and review the open source community's typical procedures regarding provenance, configuration management, sources, binaries, reusable frameworks, reusable libraries' availability for testing and use, and any other information that may impact levels of exposure to cybersecurity risks throughout the supply chain. Numerous open source solutions are currently in use by enterprises, including in integrated development environments (IDEs) and web servers. The enterprise 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 enterprise,
c. Document and monitor the distribution of software as it relates to the licensing agreement to control copying and distribution, and
d. Evaluate and periodically audit the OSS's 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 through obtaining existing and often public documents, as well

as using experience based on software update and download processes in which the enterprise may have participated.

Level(s): 2, 3

CM-11 USER-INSTALLED SOFTWARE

Supplemental C-SCRM Guidance: This control extends to the enterprise information system and network users who are not employed by the enterprise. 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 that resides in different physical locations may be subject to different cybersecurity risks throughout the supply chain, depending on the specific location of the information. Components that originate or operate from different physical locations may also be subject to different supply chain risks, depending on the specific location of origination or operations. Enterprises should manage these risks through limiting access control and 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 enterprise-defined information on enterprise-defined system components to ensure that controls are in place to protect enterprise 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 for 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 enterprise. The data map may be an overlay of any system design artifact that the enterprise 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: Enterprises should verify that the acquired hardware and software components are genuine and valid by using digitally signed components from trusted certificate authorities. Verifying components before allowing installation helps enterprises reduce cybersecurity risks throughout the supply chain.

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.

Cybersecurity supply chain contingency planning includes planning for alternative suppliers of system components, alternative suppliers of systems and services, alternative delivery routes for critical system components, and denial-of-service attacks on the supply chain. Such contingency plans help ensure that existing service providers have an effective continuity of operations plan, 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 supply chains with their own attendant cybersecurity risks. Enterprises should ensure that they understand and manage cybersecurity risks throughout the supply chain and dependencies related to the contingency planning activities as necessary.

CP-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: Enterprises should integrate C-SCRM into the contingency planning policy and related SCRM Strategy/Implementation Plan, policies, and SCRM Plan. The policy should 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: Enterprises should define and implement a contingency plan for the supply chain information systems and network to ensure that preparations are in place to mitigate the loss or degradation of data or operations. Contingencies should be put in place for the supply chain, network, information systems (especially critical components), and processes to ensure protection against compromise and 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 enterprise elements responsible for related plans.

Level(S): 2, 3

(2) *CONTINGENCY PLAN | CAPACITY PLANNING*

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

Level(s): 2, 3

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

Supplemental C-SCRM Guidance: Enterprises should ensure that the 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. Enterprises should ensure that contingency planning requirements are defined as part of the service-level agreement. The agreement may have specific terms that address critical components and functionality support in case of denial-of-service attacks to ensure the continuity of operations. Enterprises should coordinate with external service providers to identify service providers' existing contingency plan practices and build on them as required by the enterprise's mission and business needs. Such coordination will aid in cost reduction and efficient implementation. Enterprises should require their prime contractors who provide a mission- and business-critical or -enabling service or product to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 3

(4) *CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*

Supplemental C-SCRM Guidance: Ensure that critical assets (including hardware, software, and personnel) are identified and that appropriate contingency planning requirements are defined and applied to ensure the continuity of operations. 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: Enterprises should ensure that critical suppliers are included in contingency training. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

Control Enhancement(s):

(1) *CONTINGENCY TRAINING | SIMULATED EVENTS*

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

Level(s): 2, 3

CP-6 ALTERNATIVE STORAGE SITE

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

Level(s): 2, 3

Control Enhancement(s):

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

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

Level(s): 2, 3

CP-7 ALTERNATIVE PROCESSING SITE

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

Level(s): 2, 3

CP-8 TELECOMMUNICATIONS SERVICES

Supplemental C-SCRM Guidance: Enterprises should incorporate alternative telecommunication service providers for their supply chain to support critical information systems.

Level(s): 2, 3

Control Enhancement(s):

(1) *TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY AND ALTERNATIVE PROVIDERS*

Supplemental C-SCRM Guidance: The separation of primary and alternative providers supports cybersecurity resilience of the supply chain.

Level(s): 2, 3

(2) *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 ALTERNATIVE COMMUNICATIONS PROTOCOLS

Supplemental C-SCRM Guidance: Enterprises should ensure that critical suppliers are included in contingency plans, training, and testing as part of incorporating alternative communications protocol capabilities to establish supply chain resilience.

Level(s): 2, 3

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 the identification and authentication of components in addition to individuals (users) and processes acting on behalf of individuals within the supply chain network. Identification and authentication are critical to C-SCRM because they provide for the traceability of individuals, processes acting on behalf of individuals, and specific systems/components in an enterprise's supply chain network. Identification and authentication are required to appropriately manage cybersecurity risks throughout the supply chain to both reduce the risk of supply chain cybersecurity compromise and to generate evidence in case of supply chain cybersecurity compromise.

IA-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: The enterprise should – at enterprise-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 enterprise'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 enterprise 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: Enterprises should ensure that identification and requirements are defined and applied for enterprise users accessing an ICT/OT system or supply chain network. An enterprise user may include employees, individuals deemed to have the equivalent status of employees (e.g., contractors, guest researchers, etc.), and system integrators fulfilling contractor roles. Criteria such as "duration in role" can aid in defining which identification and authentication mechanisms are used. The enterprise may choose to define a set of roles and associate a level of authorization to ensure proper implementation. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 1, 2, 3

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Supplemental C-SCRM Guidance: Enterprises should implement capabilities to distinctly and positively identify devices and software within their supply chain and, once identified, verify that the identity is authentic. Devices that require unique device-to-device identification and authentication should be defined by type, device, or 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 enterprise 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 enterprise's 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 enterprise.

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 enterprise's supply chain, such as when they are transferred to the enterprise'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. Enterprises should correlate those identifiers with the enterprise-assigned identifiers for traceability and accountability. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

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

Control Enhancement(s):

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

Supplemental C-SCRM Guidance: This enhancement helps the traceability and provenance of elements within the supply chain through the coordination of identifier management among the enterprise 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 supply chain. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

Control Enhancement(s):

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

Supplemental C-SCRM Guidance: This enhancement verifies the chain of custody within the enterprise's supply chain.

Level(s): 3

(2) *AUTHENTICATOR MANAGEMENT | FEDERATED CREDENTIAL MANAGEMENT*

Supplemental C-SCRM Guidance: This enhancement facilitates provenance and chain of custody within the enterprise's 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 enterprise's supply chain for service delivery (e.g., development/integration services, product support, etc.). Enterprises should manage the establishment, auditing, use, and revocation of identification credentials and the authentication of non-enterprise users within the supply chain. Enterprises should also ensure promptness in performing identification and authentication activities, especially in the case of revocation management, to help mitigate exposure to cybersecurity risks throughout the supply chain such as those that arise due to insider threats.

Level(s): 2, 3

IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION

Supplemental C-SCRM Guidance: Enterprises should ensure that identification and authentication are defined and managed for access to services (e.g., web applications using digital certificates, services or applications that query a database as opposed to labor services) throughout the supply chain. Enterprises should ensure that they know what services are being procured and from whom. Services procured should be listed on a validated list of services for the enterprise or have compensating controls in place. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

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.

Supply chain compromises may span suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Enterprises should ensure that 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 supply chain.

IR-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: Enterprises should integrate C-SCRM into incident response policy and procedures, and related C-SCRM Strategy/Implementation Plans and Policies. The policy and procedures must provide direction for how to address supply chain-related incidents and cybersecurity incidents that may complicate or impact the supply chain. Individuals who work within specific mission and system environments need to recognize cybersecurity supply chain-related incidents. The 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 the FASC requests information relating to a particular source, covered article, or procures or an executive agency has determined that 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 1) the 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 2) the 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 supply chain cybersecurity incident. Incident information may also be shared with enterprises 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. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

In Level 2 and Level 3, procedures and enterprise-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*

Enterprises should ensure that their incident response policies and procedures provide guidance on effective information sharing of incidents and other key risk indicators in the 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 public data repositories, paid subscription services, and in-house threat intelligence teams.

Enterprises that operate 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 or covered article, or
2) An executive agency has determined that there is a reasonable basis to conclude that 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:

1) 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
2) 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: Enterprises should ensure that critical suppliers are included in incident response training. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

IR-3 INCIDENT RESPONSE TESTING

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

Level(s): 2, 3

IR-4 INCIDENT HANDLING

Supplemental C-SCRM Guidance: Suspected cybersecurity supply chain events that may trigger an organization's C-SCRM incident handling processes. Refer to Appendix G: Task 3.4 for examples of supply chain events. C-SCRM-specific supplemental guidance is provided in control enhancements.

Level(s): 1, 2, 3

Control Enhancement(s):

(1) *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. Enterprises 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

(2) *INCIDENT HANDLING | INSIDER THREATS – INTRA-ORGANIZATION*

Supplemental C-SCRM Guidance: This enhancement helps limit the exposure of C-SCRM information systems, networks, and processes to insider threats. Enterprises 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

(3) *INCIDENT HANDLING | SUPPLY CHAIN COORDINATION*

Supplemental C-SCRM Guidance: A number of enterprises may be involved in managing incidents and responses for supply chain security. After initially processing the incident and deciding on a course of action (in some cases, the action may be "no action"), the enterprise 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. Enterprises 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 supply chain cybersecurity incident handling is important for reducing exposure to cybersecurity risks throughout the supply chain. 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. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2

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

Supplemental C-SCRM Guidance: An enterprise 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: Enterprises should ensure that agreements with suppliers include requirements to track and document incidents, 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):

(1) *INCIDENT REPORTING | SUPPLY CHAIN COORDINATION*

Supplemental C-SCRM Guidance: Communications of security incident information from the enterprise to suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers and vice versa require protection. The enterprise should ensure that information is reviewed and approved for sending based on its agreements with suppliers and any relevant interagency bodies. Any escalation of or exception from this reporting should be clearly defined in the agreement. The enterprise should ensure that incident reporting data is adequately protected for transmission and received by approved individuals only. Enterprises should require their 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: The enterprise's agreements with prime contractors should specify the conditions under which a government-approved or -designated third party would be available or may be required to provide assistance with incident response, as well as the role and responsibility of that third party.

Level(s): 3

IR-8 INCIDENT RESPONSE PLAN

Supplemental C-SCRM Guidance: Enterprises 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. Enterprises should require their 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 enterprise 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). Enterprises should require their 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 enterprise. 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 exposure to cybersecurity risks throughout the supply chain, selecting C-SCRM controls, implementing those controls, and monitoring them for effectiveness.

MA-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: Enterprises should ensure that C-SCRM is included in maintenance policies and procedures and any related SCRM Strategy/Implementation Plan, SCRM Policies, and SCRM Plan(s) for all enterprise information systems and networks. With many maintenance contracts, information on mission-, enterprise-, and system-specific objectives and requirements is shared between the enterprise 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 supply chain affects upgrades, patches, the frequency of maintenance, replacement parts, and other aspects of system maintenance.

Maintenance policies should be defined for both the system and the network. The maintenance policy should reflect controls based on a risk assessment (including criticality analysis), such as remote access, the roles and attributes of maintenance personnel who have access, the frequency of updates, duration of the contract, the 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, the contract should state the source code, test cases, and other item accessibility needed to maintain a system or components.

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 Level 2 and Level 3. For example, when nonlocal maintenance is not allowed by Level 1, it should also not be allowed at Level 2 or Level 3.

The enterprise should communicate applicable maintenance policy requirements to relevant prime contractors and require that 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):

(1) *CONTROLLED MAINTENANCE |AUTOMATED MAINTENANCE ACTIVITIES*

Supplemental C-SCRM Guidance: Enterprises 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 enterprise acquires or upgrades a maintenance tool (e.g., an update to the development environment or testing tool), including during the selection, ordering, storage, and integration of the maintenance tool. The enterprise should perform continuous review and approval of maintenance tools, including those maintenance tools in use by external service providers. The enterprise should also integrate C-SCRM when evaluating replacement parts for maintenance tools. This control may be performed at both Level 2 and Level 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 enterprise 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 enterprise should verify that the media containing diagnostic and test programs that suppliers use on the enterprise's information systems operates as expected and provides only required functions. The use of media from maintenance tools should be consistent with the enterprise's policies and procedures and pre-approved. Enterprises should also ensure that the functionality does not exceed that which was agreed upon.

Level(s): 3

(3) *MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL*

Supplemental C-SCRM Guidance: The unauthorized removal of systems and network maintenance tools from the supply chain may introduce supply chain risks, such as unauthorized modification, replacement with counterfeit, or malware insertion while the tool is outside of the enterprise's control. Systems and network maintenance tools can include an integrated development environment (IDE), testing, or vulnerability scanning. For C-SCRM, it is important that enterprises should explicitly authorize, track, and audit any removal of maintenance tools. Once systems and network tools are allowed access to an enterprise/information system, they should remain the property/asset of the system owner and tracked if removed and used elsewhere in the enterprise. ICT maintenance tools

either currently in use or in storage should not be allowed to leave the enterprise'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 enterprise'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):

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

Supplemental C-SCRM Guidance: Should suppliers, developers, system integrators, external system service providers, or other ICT/OT-related service providers perform any nonlocal maintenance or diagnostic services on systems or system components, the enterprise 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 enterprise and vendor;
- Appropriate levels of sanitizing are completed to remove any enterprise-specific data residing in components; and
- Appropriate diagnostics are completed to ensure that components are sanitized, preventing malicious insertion prior to returning to the enterprise system or supply chain network.

The enterprise 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 suppliers, developers, 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 who performs a similar maintenance role and enforced through contractual agreements with their external service providers.

Level(s): 2, 3

Control Enhancement(s):

(1) *MAINTENANCE PERSONNEL | FOREIGN NATIONALS*

Supplemental C-SCRM Guidance: The 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. Enterprises should specify in agreements any restrictions or vetting requirements that pertain to foreign nationals and flow the requirements down to relevant subcontractors.

Level(s): 2, 3

MA-6 TIMELY MAINTENANCE

Supplemental C-SCRM Guidance: The enterprise should purchase spare parts, replacement parts, or alternative sources through original equipment manufacturers (OEMs), authorized distributors, or authorized resellers 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. Enterprises should obtain verification on whether the distributor or reseller is authorized. Where possible, enterprises 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 revisiting the criticality and threat analysis to identify additional risk mitigations to be used. For example, the enterprise should check the supply source for a history of counterfeits, inappropriate practices, or a criminal record. See Section 2 for criticality and threat analysis details. The enterprise should maintain a bench stock of critical OEM parts, if feasible, when the acquisition of such parts may not be accomplished within needed timeframes.

Level(s): 3

MA-7 FIELD MAINTENANCE

Supplemental C-SCRM Guidance: Enterprises 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 enterprise 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 enterprise should also report this information to the Government-Industry Data Exchange Program (GIDEP).

Supplemental C-SCRM Guidance: Tracking the failure rates of components provides useful information to the acquirer to help plan for contingencies, alternative sources of supply, and replacements. Failure rates are also useful for monitoring the 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 enterprise'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 supply chain or containing information about the enterprise's supply chain. This includes both physical and logical media, such as 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. Enterprises should ensure that media protection controls are applied to both an enterprise'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 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 also address supply chain concerns, including media in the enterprise's supply chain and throughout the SDLC.

Level(s): 1, 2

MP-4 MEDIA STORAGE

Supplemental C-SCRM Guidance: Media storage controls should include C-SCRM activities. Enterprises should specify and include in agreements (e.g., contracting language) media storage requirements (e.g., encryption) for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The enterprise 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 enterprise should incorporate C-SCRM activities when media is transported by enterprise or non-enterprise 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: Enterprises 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 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 ensuring that information is removed before the media is used, reused, or discarded. For media that contains privacy or other sensitive information (e.g., CUI), the enterprise 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.

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

PE-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: The enterprise should integrate C-SCRM practices and requirements into their own 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 supply chain have adequate protection and audit for such protection.

Level(s): 1, 2, 3

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Supplemental C-SCRM Guidance: Enterprises should ensure that only authorized individuals with a need for physical access have access to information, systems, or data centers (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 enterprise should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Authorization for non-federal employees should follow an approved protocol, which includes documentation of the authorization and specifies 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 enterprises engaged in the enterprise's supply chain. A vetting process based on enterprise-defined requirements and policy should be in place prior to granting access to the supply chain infrastructure and any relevant elements. Access establishment, maintenance, and revocation processes should meet enterprise access control policy rigor. The speed of revocation for suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers who need access to physical facilities and data centers – either enterprise-owned or external service provider-owned – should be managed in accordance with the activities performed in their contracts. Prompt revocation is critical when either individual or enterprise 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 that provid services support with physical access to the 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 security checks of facilities, enterprises should account for exfiltration risks that result 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 the enterprise.

Level(s): 2, 3

(3) *PHYSICAL ACCESS CONTROL | TAMPER PROTECTION*

Supplemental C-SCRM Guidance: Tamper protection is critical for reducing cybersecurity risk in products. The enterprise should implement validated tamper protection techniques within the supply chain. For critical products, the enterprise should require and assess whether and to what extent a supplier has implemented tamper protection mechanisms. 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 who physically access the enterprise or external service provider's facilities, data centers, information, or physical asset(s) – including via the supply chain – may be employed by the enterprise's employees, on-site or remotely located contractors, visitors, other third parties (e.g., maintenance personnel under contract with the contractor enterprise), or an individual affiliated with an enterprise in the upstream supply chain. The enterprise should monitor these individuals' activities to reduce cybersecurity risks throughout the supply chain or require monitoring in agreements.

Level(s): 1, 2, 3

PE-16 DELIVERY AND REMOVAL

Supplemental C-SCRM Guidance: This control enhancement reduces cybersecurity risks that arise during the physical delivery and removal of hardware components from the enterprise's information systems or supply chain. This includes transportation security, the validation of delivered components, and the verification of sanitization procedures. Risk-based considerations include component mission criticality as well as the development, operational, or maintenance environment (e.g., classified integration and test laboratory).

Level(s): 3

PE-17 ALTERNATIVE WORK SITE

Supplemental C-SCRM Guidance: The enterprise should incorporate protections to guard against cybersecurity risks associated with enterprise employees or contractor personnel within or accessing the supply chain infrastructure using alternative work sites. This can include third-party personnel who may also work from alternative 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 enterprise's locations. For example, enterprises should incorporate the manufacturing, warehousing, or the distribution location of information system components that are 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 enterprise should, whenever possible and practical, use asset location technologies to track systems 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 the system or component for counterfeit replacement;
b. The loss of confidentiality, integrity, or availability of the 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 C-SCRM Guidance: Enterprises should incorporate the facility location (e.g., data centers) when assessing risks 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. Enterprises should also assess whether the location of a manufacturing or distribution center could be influenced by geopolitical, economic, or other factors. For critical vendors or products, enterprises should specifically address any requirements or restrictions concerning the facility locations of the vendors (or their upstream supply chain providers) 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 activities such as security architecture, coordination with other enterprise 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, enterprises may be sharing facilities with those enterprises, have employees of these entities on the enterprise's premises, or use information systems that belong to those entities. In these and other applicable situations, enterprises should coordinate their security planning activities with these entities to ensure appropriate protection of an enterprise's processes, information systems, and systems and components traversing the supply chain. When establishing security architectures, enterprises should provide for component and supplier diversity to manage cybersecurity risks throughout the supply chain to include suppliers going out of business or stopping the production of specific components. Finally, as stated in Section 2 and Appendix C, enterprises should integrate C-SCRM controls into their Risk Response Frameworks (Level 1 and Level 2) as well as their C-SCRM Plans (Level 3).

PL-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: The security planning policy and procedures should integrate C-SCRM. This includes creating, disseminating, and updating the 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, system interfaces, and network connections. The C-SCRM policy and procedures provide inputs into and take guidance from the C-SCRM Strategy and Implementation Plan at Level 1 and the 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 enterprise 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 and Implementation Plan at Level 1 and the C-SCRM policy at Level 1 and Level 2. In addition to internal coordination, the enterprise 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 coordination and collaboration between the enterprise 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 consider 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 strategies, policies, and plans. 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: The rules of behavior apply to contractor personnel and internal agency personnel. Contractor enterprises 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 the removal of access for such individuals.

Level(s): 2, 3

PL-7 CONCEPT OF OPERATIONS

Supplemental C-SCRM Guidance: The concept of operations (CONOPS) should describe how the enterprise intends to operate the system from the perspective of C-SCRM. It should integrate C-SCRM and be managed and updated throughout the applicable system's SDLC to address cybersecurity risks throughout the supply chain.

Level(s): 3

PL-8 SECURITY AND PRIVACY ARCHITECTURES

Supplemental C-SCRM Guidance: Security and privacy architecture defines and directs the 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 that security is built-in throughout the SDLC. Enterprises should consider implementing zero-trust architectures and should 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):

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

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

The enterprise should plan for the 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 enterprise's requirements (e.g., company goes out of business or does not meet contractual obligations). Where applicable, contracts should be worded so that different parts can be

replaced with a similar model with similar prices from a different manufacturer if certain events occur (e.g., obsolescence, poor performance, production issues, etc.).

Incorporate supplier diversity for off-the-shelf (commercial or government) components during acquisition security assessments. The evaluation of alternatives should include, for example, feature parity, interoperability, commodity components, and the ability to provide multiple delivery paths. For example, having the source code, build scripts, and tests for a software component could enable an enterprise to assign someone else to maintain it, if necessary.

Level(s): 2, 3

PL-9 CENTRAL MANAGEMENT

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

Level(s): 1, 2

PL-10 BASELINE SELECTION

Supplemental C-SCRM Guidance: Enterprises should include C-SCRM controls in their control baselines. Enterprises should identify and select C-SCRM controls based on the 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 enterprise 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 enterprise level and not directed at individual information systems." Those controls apply to the entire enterprise (i.e., federal agency) and support the enterprise's overarching information security program. Program management controls support and provide input and feedback to enterprise-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 similar is responsible for implementing program management controls. Section 3 provides guidance on the C-SCRM PMO and its functions and responsibilities.

PM-2 INFORMATION SECURITY PROGRAM LEADERSHIP ROLE

Supplemental C-SCRM Guidance: The 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-enterprise coordination and collaboration with other applicable senior personnel within the enterprise, such as the CIO, the head of facilities/physical security, and the risk executive (function). This coordination should occur regardless of the specific department and agency enterprise structure and specific titles of relevant senior personnel. The coordination could be executed by the 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 enterprise'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 enterprise should also integrate C-SCRM requirements into major IT investments to ensure that funding is appropriately allocated through the capital planning and investment request process. For example, should an RFID infrastructure be required to enhance C-SCRM to secure and improve the inventory or logistics management efficiency of the enterprise's supply chain, appropriate IT investments would likely be required to ensure successful planning and implementation. Other examples include any investment into the development or test environment for critical components. In such cases, 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. Organizations should develop POA&Ms based on C-SCRM assessment reports. POA&M should be used by organizations to describe planned actions to correct the deficiencies in C-SCRM controls identified during assessment and the continuous monitoring of progress against those actions.

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 the enterprise's inability to identify system and supplier criticality, which would result in an inability to conduct C-SCRM activities. To ensure that all applicable suppliers are identified and categorized for criticality, enterprises should include relevant supplier information in the system inventory and maintain its currency and accuracy. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

PM-6 MEASURES OF PERFORMANCE

Supplemental C-SCRM Guidance: Enterprises should use measures of performance to track the implementation, efficiency, effectiveness, and impact of C-SCRM activities. The C-SCRM PMO is responsible for creating C-SCRM measures of performance in collaboration with other applicable stakeholders to include identifying the 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: The risk management strategy should address cybersecurity risks throughout the supply chain. Section 2, Appendix C, and Appendix D of this document provide guidance on integrating C-SCRM into the 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: The enterprise's mission and business processes should address cybersecurity risks throughout the supply chain. When addressing mission and business process definitions, the enterprise 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 a 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: The enterprise should implement a process to ensure that organizational plans for conducting supply chain risk testing, training, and monitoring activities associated with organizational systems are maintained. The 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. The 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: A threat awareness program should include threats that emanate from the supply chain. When addressing supply chain threat awareness, knowledge should be shared between stakeholders within the boundaries of the enterprise's information sharing policy. The 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: The policy and procedures for controlled unclassified information (CUI) on external systems should include protecting relevant supply chain information. Conversely, it should include protecting agency information that resides in external systems because such external systems are part of the agency supply chain.

Level(s): 2

PM-18 PRIVACY PROGRAM PLAN

Supplemental C-SCRM Guidance: The privacy program plan should include C-SCRM. Enterprises should require their 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: The privacy program leadership role should be included as a stakeholder in applicable C-SCRM initiatives and activities.

Level(s): 1

PM-20 DISSEMINATION OF PRIVACY PROGRAM INFORMATION

Supplemental C-SCRM Guidance: The dissemination of privacy program information should be protected from cybersecurity risks throughout the supply chain.

Level(s): 1, 2

PM-21 ACCOUNTING OF DISCLOSURES

Supplemental C-SCRM Guidance: An accounting of disclosures should be protected from cybersecurity risks throughout the supply chain.

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 cybersecurity risks related to PII throughout the supply chain.

Level(s): 1, 2

PM-23 DATA GOVERNANCE BODY

Supplemental C-SCRM Guidance: Data governance body is a stakeholder in C-SCRM and 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: Supply chain-related cybersecurity risks to personally identifiable information should be addressed by the 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 cybersecurity risks throughout the supply chain. Enterprises 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 cybersecurity risks throughout the supply chain.

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 detailed 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 enterprise. Section 2 and Appendix C provide detailed guidance for C-SCRM roles and responsibilities.

Level(s): 1

PM-30 SUPPLY CHAIN RISK MANAGEMENT STRATEGY

Supplemental C-SCRM Guidance: The 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 enterprise 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 enterprise should select and document common C- SCRM controls that should address the enterprise, program, and system-specific needs. These controls should be iteratively integrated into the C-SCRM

Policy at Level 1 and Level 2, as well as the 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: The continuous monitoring strategy and program should integrate C-SCRM controls at Levels 1, 2, and 3 in accordance with the 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, including cybersecurity risks throughout the supply chain. The application of this control should include the explicit incorporation of cybersecurity 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 who have access to an enterprise's supply chain should be covered by the enterprise'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. Enterprises should also work with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to ensure that they apply appropriate security controls to the personnel who interact with the enterprise's supply chain, as appropriate.

PS-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: At each level, the personnel security policy and procedures and the 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 regard 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 that provide supporting supply chain activities.

Level 2: Applicable roles include program executive and individuals (e.g., non-federal employees, including contractors) within the acquirer enterprise who are 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 the 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 the acquirer and these parties (e.g., contract).

The enterprise 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 risk, 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 enterprise policies. Screening requirements should be incorporated into agreements and flow down to sub-tier contractors.

Level(s): 2, 3

PS-6 ACCESS AGREEMENTS

Supplemental C-SCRM Guidance: The enterprise should define and document access agreements for all contractors or other external personnel who may need to access the enterprise'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 enterprise's information security policy and may need to specify additional restrictions, such as allowing access during specific timeframes, from specific locations, or only by personnel who have satisfied additional vetting requirements. The enterprise 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 enterprise 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 enterprise, 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 enterprise 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 who have access to the enterprise's information systems and networks must meet the same personnel security requirements as enterprise personnel. Examples of such third-party personnel can include the system integrator, developer, supplier, external service provider used for delivery, contractors or service providers who are using the ICT/OT systems, or supplier maintenance personnel brought in to address component technical issues not solvable by the enterprise 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 enterprise should keep in mind that some suppliers have comprehensive security and privacy practices and systems that may go above and beyond the enterprise's requirements. The enterprises should work with suppliers to understand the extent of their privacy practices and how they meet the enterprise's needs.

PT-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: Enterprises should ensure that supply chain concerns are included in PII processing and transparency policies and procedures, as well as the 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 the purpose, scope, roles, responsibilities, management commitment, coordination among enterprise 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 that contracts state what PII data will be shared, which contractor personnel may have access to the PII, controls protecting PII, 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 requirements.

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

c. The enterprise 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.

This document provides guidance for managing an enterprise's cybersecurity risk in supply chains and expands this control to integrate assessments of cybersecurity risk in supply chains, 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. The system-level risk assessment should include both the supply chain infrastructure (e.g., development and testing environments and delivery systems) and the information system/components traversing the supply chain. System-level risk assessments significantly intersect with the SDLC and should complement the enterprise's 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 on the mission, if compromised. The policy should include supply chain-relevant cybersecurity roles that are applicable to performing and coordinating risk assessments across the enterprise (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, security categorization for C-SCRM should be based on the criticality analysis that 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. The data to be reviewed and collected includes C-SCRM-specific roles, processes, and the 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 enterprise 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 with 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 enterprise'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 that they provide through the cybersecurity supply chain. Vulnerability monitoring activities should take place at all three levels of the enterprise. Scoping vulnerability monitoring activities requires enterprises to consider suppliers as well as their sub-suppliers. Enterprises, where applicable and appropriate, may consider providing customers with a Vulnerability Disclosure Report (VDR) to demonstrate proper and complete vulnerability assessments for components listed in SBOMs. The VDR should include the analysis and findings describing the impact (or lack of impact) that the reported vulnerability has on a component or product. The VDR should also contain information on plans to address the CVE. Enterprises should consider publishing the VDR within a secure portal available to customers and signing the VDR with a trusted, verifiable, private key that includes a timestamp indicating the date and time of the VDR signature and associated VDR. Enterprises should also consider establishing a separate notification channel for customers in cases where vulnerabilities arise that are not disclosed in the VDR. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

Control Enhancement(s):

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

Supplemental C-SCRM Guidance: Enterprises that monitor the supply chain for vulnerabilities should express the 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 at which the monitoring takes place (e.g., sub-supplier). Where possible, a component inventory (e.g., hardware, software) may aid enterprises in capturing the breadth and depth of the products/components within their supply chain that may need to be monitored and scanned for vulnerabilities.

Level(s): 2, 3

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

Supplemental C-SCRM Guidance: Enterprises should track trends in vulnerabilities to components within the supply chain over time. This information may help enterprises develop procurement strategies that reduce risk exposure density within the supply chain.

Level(s): 2, 3

RA-7 RISK RESPONSE

Supplemental C-SCRM Guidance: Enterprises should integrate capabilities to respond to cybersecurity risks throughout the supply chain into the enterprise's overall response posture, ensuring that these responses are aligned to and fall within the boundaries of the enterprise'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: Enterprises should complete a criticality analysis as a prerequisite input to assessments of cybersecurity supply chain risk management activities. First, enterprises should complete a criticality analysis as part of the Frame step of the C-SCRM Risk Management Process. Then, findings generated in the 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, enterprises should employ it iteratively throughout the SLDC and concurrently across the three levels. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should also refer to Appendix F to supplement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 1, 2, 3

RA-10 THREAT HUNTING

Supplemental C-SCRM Guidance: The C-SCRM threat hunting activities should supplement the enterprise's internal threat hunting activities. As a critical part of the cybersecurity supply chain risk management process, enterprises should actively monitor for threats to their supply chain. This requires a collaborative effort between C-SCRM and other cyber defense-oriented functions within the enterprise. Threat hunting capabilities may also be provided via a shared services enterprise, especially when an enterprise lacks the resources to perform threat hunting activities themselves. Typical activities include information sharing with peer enterprises and actively consuming threat intelligence sources (e.g., like those available from Information Assurance and Analysis Centers [ISAC[and Information Assurance and Analysis Organizations [ISAO]). These activities can help identify and flag indicators of increased cybersecurity risks throughout the supply chain that may be of concern, such as cyber incidents, mergers and acquisitions, and Foreign Ownership, Control, or Influence (FOCI). Supply chain threat intelligence should seek out threats to the enterprise's suppliers, as well as information systems, system components, and the raw inputs that they provide. The intelligence gathered enables enterprises 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.

Enterprises acquire ICT/OT products and services through system and services acquisition. These controls address the activities of acquirers, suppliers, developers, system integrators, external system service providers, other ICT/OT-related service providers, and related upstream supply chain relationships. They address both the physical and logical aspects of 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]. This document adds further detail and refinement to these controls.

SA-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: The 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 the 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 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 enterprise'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 enterprise'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, enterprises 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 that 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 enterprises understand these changes and use the obtained information to inform their C-SCRM activities. Enterprises can obtain the 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. Additionally, Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity.

Level(s): 1, 2, 3

SA-2 ALLOCATION OF RESOURCES

Supplemental C-SCRM Guidance: The enterprise 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 enterprise should ensure that C-SCRM activities are integrated into the SDLC for both the enterprise 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 the logical delivery of systems and components. See Section 2 and Appendix C for further guidance on SDLC. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 1, 2, 3

SA-4 ACQUISITION PROCESS

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

1. Enterprises are to establish baseline and tailorable 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:
    a. C-SCRM requirements that cover regulatory mandates (e.g., the 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 that provide assurance that the contractor is sufficiently responsible, capable, and trustworthy.
    b. Requirements for critical elements in the supply chain to demonstrate the capability to remediate emerging vulnerabilities based on open source information and other sources.
    c. Requirements for managing intellectual property ownership and responsibilities for elements such as software code; data and information; the manufacturing, development, or integration environment; designs; and proprietary processes when provided to the enterprise for review or use.
    d. Requirements that address the expected life span of the product or system, any element(s) that may be in a critical path based on their life span, and what is required when end-of-life is near or has been reached. Enterprises should conduct research or solicit information from bidders or existing providers under contract to understand what end-of-life options exist (e.g., replace, upgrade, migrate to a new system, etc.).
    e. Articulate any circumstances when secondary market components may be permitted.

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

2. Enterprises should:

   a. Establish a plan for the acquisition of spare parts to ensure adequate supply, and execute the plan if or when applicable;

   b. Establish a plan for the acquisition of alternative sources of supply as may be necessary during continuity events or if/when a disruption to the supply chain occurs;

   c. 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 enterprises within their supply chains.

3. Establish and maintain verification procedures and acceptance criteria for delivered products and services, which include but are not limited to:

   a. Accepting COTS and GOTS products without verification, as authorized by the enterprise (e.g., approved products lists)

   b. Supplier validation of developmental and COTS software and hardware information system vulnerabilities

4. Ensure that the continuous monitoring plan includes supply chain aspects in its criteria, such as including the monitoring of functions, ports, and protocols in use. See Section 2 and Appendix C.

5. Ensure that 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. These include but are not limited to monitoring software development infrastructure for vulnerabilities (e.g., DevSecOps pipelines, software containers, and code repositories/shares).

6. 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.

7. Review and confirm sustained compliance with the terms and conditions of the agreement on an ongoing basis.

Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 1, 2, 3

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

Control Enhancement(s):

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

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

Level(s): 3

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

Supplemental C-SCRM Guidance: This control enhancement requires that the enterprise 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

(3) *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). Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity.

Level(s): 3

SA-8 SECURITY AND PRIVACY ENGINEERING PRINCIPLES

Supplemental C-SCRM Guidance: The following security engineering techniques are helpful for managing cybersecurity risks throughout the supply chain.

a. Anticipate the maximum possible ways that the ICT/OT product or service can be misused or 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 enterprise's risk tolerance, as determined by risk assessments (see Section 2 and Appendix C).
c. Document and gain management acceptance and approval for risk that is 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 cybersecurity vulnerabilities, such as 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 they are 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 supply chain and the systems/components traversing the supply chain during delivery.
h. Design relevant validation mechanisms to be used during implementation and operation.

Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 1, 2, 3

SA-9 EXTERNAL SYSTEM SERVICES

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

Control Enhancement(s):

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

Supplemental C-SCRM Guidance: See Appendices C and D. Departments and agencies should refer to Appendix E and Appendix F to implement guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity.

Level(s): 2, 3

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

Supplemental C-SCRM Guidance: Relationships with providers[37] should meet the following supply chain security requirements:

a. The requirements definition is complete and reviewed for accuracy and completeness, including the assignment of criticality to various components and defining operational concepts and associated scenarios for intended and unintended use.
b. Requirements are based on needs, relevant compliance drivers, criticality analysis, and assessments of cybersecurity risks throughout the supply chain.
c. Cyber supply chain threats, vulnerabilities, and associated risks are identified and documented.
d. Enterprise 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. The consequences of non-compliance with C-SCRM requirements and information system security requirements are defined and documented.
f. There is a clear delineation of accountabilities, roles, and responsibilities between contractors when multiple disparate providers are engaged in supporting a system or mission and business function.
g. The requirements detail 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.
h. Establish negotiated agreements for relationship termination to ensure a safe and secure termination, such as removing data from cloud environments.

Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 1, 2, 3

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

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

Level(s): 3

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

[37] In the context of this enhancement, providers may include suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

Supplemental C-SCRM Guidance: The location may be under the control of the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Enterprises 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 that appropriate protections are in place to address associated C-SCRM risk.

Level(s): 3

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Supplemental C-SCRM Guidance: Developer configuration management is critical for reducing cybersecurity risks throughout the supply chain. By conducting configuration management activities, developers reduce the 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. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

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 or security processes. When the acquirer has control over the application and 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), as well as the effectiveness of testing techniques. Enterprises may also require third-party testing as part of developer security testing. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

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 the enterprise's efforts to effectively mitigate cybersecurity risks throughout the supply chain. The enterprise should apply national and international standards and best practices when implementing this control. Using existing standards promotes consistency of implementation, reliable and defendable processes, and interoperability. The enterprise'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. The use of automated tools aids thoroughness, efficiency, and the scale of analysis that helps address cybersecurity risks that arise in relation to the development process throughout the supply chain. Additionally, the output of such activities and tools provides useful inputs for C-SCRM processes, as described in Section 2 and Appendix C. This control has applicability to the internal enterprise's processes, information systems, and networks as well as applicable system integrators' processes, systems, and networks. Departments and agencies should refer to Appendix

F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

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

Control Enhancement(s):

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

Supplemental C-SCRM Guidance: This enhancement identifies critical components within the information system, which 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

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

Supplemental C-SCRM Guidance: This enhancement provides threat modeling and vulnerability analysis for the relevant federal agency and contractor products, applications, information systems, and networks. Performing this analysis will help integrate C-SCRM into code refinement and modification activities. See the 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)

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

Supplemental C-SCRM Guidance: This enhancement encourages developers to reuse the 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 the 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 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) the individuals responsible for selecting system and network components incorporate C-SCRM when choosing such components. Developer training should also cover training for secure coding and the use of tools to find vulnerabilities in software. Refer to Appendix F for additional guidance on security for critical software.

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. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity.

Level(s): 2, 3

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

SA-20 CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS

Supplemental C-SCRM Guidance: The enterprise may decide, based on their assessments of cybersecurity risks throughout the supply chain, that they require customized development of certain critical components. This control provides additional guidance on this activity. Enterprises should work with suppliers and partners to ensure that critical components are identified. Organizations should ensure that they have a continued ability to maintain custom-developed critical software components. For example, having the source code, build scripts, and tests for a software component could enable an organization to have someone else maintain it if necessary.

Level(s): 2, 3

SA-21 DEVELOPER SCREENING

Supplemental C-SCRM Guidance: The enterprise should implement screening processes for their internal developers. For system integrators who may be providing key developers that address critical components, the enterprise should ensure that appropriate processes for developer screening have been used. The 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. Enterprises 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 reduces cybersecurity risks in the supply chain. In the case of unsupported system components, the enterprise should use authorized resellers or distributors with an ongoing relationship with the supplier of the unsupported system components.

When purchasing alternative sources for continued support, enterprises should acquire directly from vetted original equipment manufacturers (OEMs) or their authorized distributors and resellers. Decisions about

using alternative sources require input from the enterprise's engineering resources regarding the differences in alternative component options. For example, if an alternative is to acquire an open source software component, the enterprise should identify the open source community development, test, acceptance, and release processes. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

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 enterprise'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 enterprise's systems and to connect to the internet, other ICT/OT within the enterprise, contractor systems, and – occasionally – supplier systems. An enterprise'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 cybersecurity risks throughout the supply chain in relation to the enterprise's processes, systems, and networks. Enterprise-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 enterprise entities within the enterprise, as well as the communications methods, external connections, and processes used between the enterprise 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 enterprise 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. Enterprises may either share too much and increase their risk or share too little and make it difficult for suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to be efficient in their service delivery. The enterprise should work with developers to define a structure or process for information sharing, including the data shared, the method of sharing, and to whom (the specific roles) the information 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):

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

Supplemental C-SCRM Guidance: The enterprise 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 enterprise 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 enterprise, supplier systems and networks, and the SDLC. Appropriate vulnerability, threat, and risk assessments should be performed to ensure proper boundary protections for supply chain components and supply chain information flow. The vulnerability, threat, and risk assessments can aid in scoping boundary protection to a relevant set of criteria and help manage associated costs. For contracts with external service providers, enterprises 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. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2

Control Enhancement(s):

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

Supplemental C-SCRM Guidance: The enterprise should provide separation and isolation of development, test, and security assessment tools and operational environments and relevant monitoring tools within the enterprise'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. Enterprises should require their 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 and isolation mechanisms or techniques.

Level(s): 3

Related Controls: SR-3(3)

(2) *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)

(3) *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: The 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 enterprise confidentiality and integrity requirements. The degree of protection should be based on the sensitivity of information to be transmitted and the relationship between the enterprise and the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

SC-18 MOBILE CODE

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

Level(s): 3

Control Enhancement(s):

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

Supplemental C-SCRM Guidance: The enterprise 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 installation 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 and 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. The enhanced portability of platform-independent applications enables enterprises to switch external service providers more readily in the event that one becomes compromised, thereby reducing vendor-dependent cybersecurity risks. This is especially relevant for critical applications on which multiple systems may rely.

Level(s): 2, 3

SC-28 PROTECTION OF INFORMATION AT REST

Supplemental C-SCRM Guidance: The enterprise should include provisions for the 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 enterprise 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. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

Related Controls: SR-3(3)

SC-29 HETEROGENEITY

Supplemental C-SCRM Guidance: Heterogeneity techniques include the 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 supply chain cybersecurity compromise. In case of a supply chain cybersecurity compromise, an alternative source of supply will allow the enterprises to more rapidly switch to an alternative system/component that may not be affected by the compromise. Addtionally, 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, the concealment of location, randomly changing the fake location used, and randomly changing or shifting information storage into alternative servers or storage mechanisms.

Level(s): 2, 3

Control Enhancement(s):

(1) *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 enterprise should employ techniques to introduce randomness into enterprise operations and assets in the enterprise's systems or networks (e.g., randomly switching among several delivery enterprises or routes, or changing the time and date of receiving supplier software updates if previously predictably scheduled).

Level(s): 2, 3

(2) *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 enterprise may leverage such techniques within the their information systems and networks to create uncertainty about the activities targeted by adversaries. Establishing a few process changes and randomizing their use – 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

(3) *CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION*

Supplemental C-SCRM Guidance: The enterprise can convey misleading information as part of concealment and misdirection efforts to protect the information system being developed and the enterprise's systems and networks. Examples of such efforts in security include honeynets or virtualized environments. Implementations can be leveraged to convey misleading information. These may be considered advanced techniques that require experienced resources to effectively implement them. If an enterprise decides to use honeypots, it should be done in concert with legal counsel or following the enterprise's policies.

Level(s): 2, 3

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

Supplemental C-SCRM Guidance: The enterprise may employ various concealment and misdirection techniques to protect information about the information system being developed and the enterprise's information systems and networks. For example, the delivery of critical components to a central or trusted third-party depot can be used to conceal or misdirect any information regarding the component's use or the enterprise 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 a potential loss of confidentiality of the component or its use, condition, or 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 enterprise's systems and networks and across the SDLC. The enterprise should ensure that these techniques are applied in both contexts. Development, manufacturing, configuration management, test, maintenance, and operations can use distributed processing and storage. This control applies to the entity responsible for processing and storage functions or related infrastructure, to include federal agencies and contractors. As such, this control applies to the federal agency and applicable supplier information systems and networks. Enterprises should require their 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 enterprise 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 enterprise 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 ALTERNATIVE 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 alternative 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 cybersecurity risks throughout the supply chain. The insertion of malicious code and counterfeits are two primary examples of cybersecurity risks throughout the supply chain, both of which can at least partially be addressed by deploying system and information integrity controls. Enterprises should ensure that adequate system and information integrity protections are part of C-SCRM.

SI-1 POLICY AND PROCEDURES

Supplemental C-SCRM Guidance: The enterprise 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, components, and the underlying information systems and networks is critical for managing cybersecurity risks throughout the supply chain. The insertion of malicious code and counterfeits are two primary examples of cybersecurity risks throughout the supply chain, 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: The output of flaw remediation activities provides useful input into the ICT/OT SCRM processes described in Section 2 and Appendix C. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2, 3

Control Enhancement(s):

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

Supplemental C-SCRM Guidance: The enterprise 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 non-critical 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 that originate directly from the OEM unless specifically deployed by the acquirer, such as with a centralized patch management process. Departments and agencies should refer to Appendix F to

implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2

SI-3 MALICIOUS CODE PROTECTION

Supplemental C-SCRM Guidance: Because the majority of code operated in federal systems is not developed by the Federal Government, malicious code threats often originate from the supply chain. This controls applies to the federal agency and contractors with code-related responsibilities (e.g., developing code, installing patches, performing system upgrades, etc.), as well as applicable contractor information systems and networks. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

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 vulnerabilities that result from past supply chain cybersecurity 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. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 1, 2, 3

Control Enhancement(s):

(1) *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 supply chain cybersecurity vulnerabilities that require mitigation or compromises.

Level(s): 2, 3

(2) *SYSTEM MONITORING | RISK FOR INDIVIDUALS*

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

Level(s): 2, 3

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Supplemental C-SCRM Guidance: The enterprise should evaluate security alerts, advisories, and directives for cybersecurity supply chain impacts and follow up if needed. US-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. Enterprises should ensure that 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. Enterprises should provide direction or guidance as to what actions are to be taken in response to sharing such an alert, advisory, or directive. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

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 products, applications, 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 control applies to federal agencies and applicable supplier information systems and networks. When purchasing an ICT/OT product, an enterprise should perform due diligence to understand what a supplier's integrity assurance practices are. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

Related Controls: SR-3(3)

Control Enhancement(s):

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

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

Level(s): 2, 3

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

Supplemental C-SCRM Guidance: The enterprise should ensure that code authentication mechanisms, such as digital signatures, are implemented to ensure 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 the sensitive and proprietary information of a system integrator, supplier, or external service provider 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 the sensitive information of a federal agency. In this instance, enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2, 3

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. The supplemental guidance below expands upon the SR controls and provides further information and context for their application. This is a new family in SP 800-53, Rev. 5, and guidance already exists in that publication. This document (NIST SP 800-161, Rev. 1) includes all SR control enhancements from SP 800-53, Rev. 5, and the following SR controls and control enhancements have been added to NIST SP 800-53, Rev. 5 [SR-13]. Readers should consult NIST SP 800-53, Rev. 5 SR controls together with the controls in this section.

SR-1 POLICY AND PROCEDURES

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

C-SCRM plans should be developed as a standalone document and only integrated into existing system security plans if enterprise 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. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity.

Level(s): 1, 2, 3

Control Enhancement(s):

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

Supplemental C-SCRM Guidance: Enterprises should diversify their supply base, especially for critical ICT/OT products and services. As a part of this exercise, the enterprise should attempt to identify

single points of failure and risk among primes and lower-level entities in the supply chain. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis.

Level(s): 2, 3

Related Controls: RA-9

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

Supplemental C-SCRM Guidance: Enterprises should require their 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. As part of procurement requirements, enterprises should include the need for suppliers to flow down controls to subcontractors throughout the SDLC. As part of market research and analysis activities, enterprises should conduct robust due diligence research on potential suppliers or products, as well as their upstream dependencies (e.g., fourth- and fifth-party suppliers), which can help enterprises avoid single points of failure within their supply chains. The results of this research can be helpful in shaping the sourcing approach and refining requirements. An evaluation of the cybersecurity risks that arise from a supplier, product, or service should be completed prior to the contract award decision to ensure that 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 documented for systems, system components, and associated data throughout the SDLC. Enterprises should consider producing SBOMs for applicable and appropriate classes of software, including purchased software, open source software, and in-house software. SBOMs should be produced using only NTIA-supported SBOM formats that can satisfy [NTIA SBOM] EO 14028 NTIA minimum SBOM elements. Enterprises producing SBOMs should use [NTIA SBOM] minimum SBOM elements as framing for the inclusion of primary components. SBOMs should be digitally signed using a verifiable and trusted key. SBOMs can play a critical role in enabling organizations to maintain provenance. However, as SBOMs mature, organizations should ensure they do not deprioritize existing C-SCRM capabilities (e.g., vulnerability management practices, vendor risk assessments) under the mistaken assumption that SBOM replaces these activities. SBOMs and the improved transparency that they are meant to provide for organizations are a complementary, not substitutive, capability. Organizations that are unable to appropriately ingest, analyze, and act on the data that SBOMs provide likely will not improve their overall C-SCRM posture. Federal agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity.

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. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity.

Level(s): 1, 2, 3

Related Controls: SA Control Family

SR-6 SUPPLIER ASSESSMENTS AND REVIEWS

Supplemental C-SCRM Guidance: In general, an enterprise should consider any information pertinent to the security, integrity, resilience, quality, trustworthiness, or authenticity of the supplier or their provided services or products. Enterprises should consider applying this information against a consistent set of core baseline factors and assessment criteria to facilitate equitable comparison (between suppliers and over time). Depending on the specific context and purpose for which the assessment is being conducting, the enterprise 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 the enterprise's supplier assessments. Departments and agencies should refer to Appendix E for further guidance concerning baseline risk factors and the documentation of assessments and Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

SR-7 SUPPLY CHAIN OPERATIONS SECURITY

Supplemental C-SCRM Guidance: The 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 enterprise's supply chain or an element within the supply chain, or when the nature of the enterprise's mission or business operations, its information, and/or its service/product offerings make it a more attractive target for an adversarial threat.

Level(s): 2, 3

SR-8 NOTIFICATION AGREEMENTS

Supplemental C-SCRM Guidance: At minimum, enterprises should require their suppliers to establish notification agreements with entities within their supply chain that have a role or responsibility related to that critical service or product. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

Related Controls: RA-9

SR-9 TAMPER RESISTANCE AND DETECTION

Supplemental C-SCRM Guidance: Enterprises 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. The C-SCRM PMO can help identify critical components, especially those that are used by multiple missions, functions, and systems within an enterprise. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

Level(s): 2, 3

Related Controls: RA-9

SR-10 INSPECTION OF SYSTEMS OR COMPONENTS

Supplemental C-SCRM Guidance: Enterprises 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. Enterprises should require their 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. The 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 enterprise.

Level(s): 2, 3

Related Controls: RA-9

SR-11 COMPONENT AUTHENTICITY

Supplemental C-SCRM Guidance: The development of anti-counterfeit policies 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 or clauses, and counterfeit reporting processes to enterprises, such as GIDEP and/or other appropriate enterprises. Where applicable and appropriate, the policy should also address the development and use of a qualified bidders list (QBL) and/or qualified manufacturers list (QML). This helps prevent counterfeits through the use of authorized suppliers, wherever possible, and their integration into the organization's supply chain [CISA SCRM WG3]. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.

Level(s): 1, 2, 3

Control Enhancement(s):

(1) *COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING*

Supplemental C-SCRM Guidance: The 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 enterprise. 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 enterprise 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: Enterprises 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. The C-SCRM PMO can help identify critical components, especially those used by multiple missions, functions, and systems within an enterprise.

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 inventory of suppliers that:

   1. Accurately and minimally reflects the organization's tier one suppliers that may present a cybersecurity risk in the supply chain [Assignment: organization-defined parameters for determining tier one supply chain];

   2. Is at the level of granularity deemed necessary for assessing criticality and supply chain risk, tracking, and reporting;

   3. Documents the following information for each tier one supplier (e.g., prime contractor): review and update supplier inventory [Assignment: enterprise-defined frequency].

      i. Unique identify for procurement instrument (i.e., contract, task, or delivery order);
      ii. Description of the supplied products and/or services;
      iii. Program, project, and/or system that uses the supplier's products and/or services; and
      iv. Assigned criticality level that aligns to the criticality of the program, project, and/or system (or component of system).

b. Review and update the supplier inventory [Assignment: enterprise-defined frequency].

Supplemental C-SCRM Guidance: Enterprises 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, and the enterprise's level of dependency on the supplier. Enterprises should use criticality analysis to help determine which products and services are critical to determine the 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 B: 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 B-1 indicates those controls that are defined in [NIST SP 800-53, Rev. 5]. Low baseline requirements are deemed to be relevant to C-SCRM. Some C-SCRM controls were added to this control set 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 enterprise-wide activity that requires the selection and implementation of controls at the enterprise, mission and business, and operational levels (Levels 1, 2, and 3 of the enterprise according to [NIST SP 800-39]), Table B-1 indicates the enterprise levels at which the controls should be implemented. C-SCRM controls and control enhancements not in [NIST SP 800-53, Rev. 5] are noted with an asterisk next to the control identifier, viz., MA-8 and SR-13.

Table B-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	x
AC-3	**Access Enforcement**	x	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	x
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	

Control Identifier	Control (or Control Enhancement) Name	C-SCRM Baseline	Flow Down Control	Levels		
				1	2	3
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		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	x
AU-3	**Content of Audit Records**	x	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 Non-technical 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	x
AU-13	**Monitoring for Information Disclosure**		x		x	x
AU-14	**Session Audit**		x		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(3)	*Continuous Monitoring | Trend Analyses*					x
CM-1	**Policy and Procedures**	x		x	x	x
CM-2	**Baseline Configuration**	x	x		x	x
CM-2(6)	*Baseline Configuration | Development and Test Environments*				x	x
CM-3	**Configuration Change Control**		x		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

Control Identifier	Control (or Control Enhancement) Name	C-SCRM Baseline	Flow Down Control	Levels 1	2	3
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	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	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

Control Identifier	Control (or Control Enhancement) Name	C-SCRM Baseline	Flow Down Control	Levels		
				1	2	3
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	x
CP-3(1)	*Contingency Training | Simulated Events*				x	x
CP-4	**Contingency Plan Testing**	x			x	x
CP-6	**Alternative Storage Site**				x	x
CP-6(1)	*Alternative Storage Site | Separation from Primary Site*				x	x
CP-7	**Alternative Processing Site**				x	x
CP-8	**Telecommunications Services**				x	x
CP-8(3)	*Telecommunications Services | Separation of Primary and Alternative Providers*				x	x
CP-8(4)	*Telecommunications Services | Provider Contingency Plan*				x	x
CP-11	**Alternative Communications Protocols**				x	x
IA-1	**Policy and Procedures**	x		x	x	x
IA-2	**Identification and Authentication (Organizational Users)**	x	x	x	x	x
IA-3	**Device Identification and Authentication**			x	x	x
IA-4	**Identifier Management**	x	x		x	x
IA-4(6)	*Identifier Management | Cross-organization Management*			x	x	x
IA-5	**Authenticator Management**	x	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	x
IR-1	**Policy and Procedures**	x	x	x	x	x
IR-2	**Incident Response Training**	x	x		x	x
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(3)	*Incident Reporting | Supply Chain Coordination*		x			x
IR-7(2)	*Incident Response Assistance | Coordination with External Providers*		x			x

Control Identifier	Control (or Control Enhancement) Name	C-SCRM Baseline	Flow Down Control	Levels		
				1	2	3
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(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	**Alternative 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	x
PM-6	**Measures of Performance**			x	x	
PM-7	**Enterprise Architecture**			x	x	

Control Identifier	Control (or Control Enhancement) Name	C-SCRM Baseline	Flow Down Control	Levels		
				1	2	3
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	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	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

Control Identifier	Control (or Control Enhancement) Name	C-SCRM Baseline	Flow Down Control	Levels		
				1	2	3
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(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(2)	*Denial-of-service Protection | Capacity, Bandwidth, and Redundancy*				x	
SC-7	**Boundary Protection**	x	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	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

				Levels		
Control Identifier	**Control (or Control Enhancement) Name**	**C-SCRM Baseline**	**Flow Down Control**	**1**	**2**	**3**
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(1)	*Out-of-band Channels | Ensure Delivery and Transmission*				x	x
SC-38	**Operations Security**				x	x
SC-47	**Alternative Communications Paths**			x	x	x
SI-1	**Policy and Procedures**	x		x	x	x
SI-2	**Flaw Remediation**	x	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	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	x
SI-7	**Software, Firmware, and Information Integrity**	x	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

APPENDIX C: RISK EXPOSURE FRAMEWORK[38]

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. The 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 enterprises have a more comprehensive understanding of the various types of threat events that can occur and lay the groundwork for analyzing the likelihood and impact that a specific event or events would have on an enterprise. Conducting this analysis is a useful way to discover gaps in controls and to identify and prioritize appropriate mitigating strategies.[39]

Threat scenarios are generally used in two ways:

1. To translate the often disconnected information garnered from a risk assessment, 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 enterprises discover dependencies and additional vulnerabilities that require mitigation and are used for training.

2. To determine the impact that a successful exercise of a specific vulnerability would have on the enterprise and identify the benefits of mitigating strategies.

Threat scenarios serve as a critical component of the enterprise's cybersecurity supply chain risk management process described in Appendix G of this publication. An enterprise 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 enterprise 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 that represents the conclusion of an enterprise's level of exposure to cybersecurity risks throughout the supply chain.

Once a risk determination has been made, the enterprise will determine a path for responding to the risk using the Risk Exposure Framework. Within the Risk Exposure Framework, enterprises will document the threat scenario, the risk analysis, the identified 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 enterprises to develop a tailored Risk Exposure Framework for potential and identified threats that best suits their needs. It contains six examples of how this framework may be used. The examples differ slightly in their implementation of the framework so as to show how the

[38] Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.
[39] Additional example threat scenarios and threat lists can be found in the ICT SCRM Task Force: Threat Scenarios Report (v3), August 2021, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf. This report leveraged the 2015 version of NIST SP 800-161.

framework may be tailored by an enterprise. Each example identifies one or more vulnerabilities, describes a specific threat source, identifies the expected impact on the enterprise, and proposes [SP 800-161, Rev. 1] C-SCRM controls that would help mitigate the resulting risk.

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 enterprise applicability, level of detail, and other constraints.
- Identify resources to be used, including personnel, time, and equipment.
- Define a Risk Exposure Framework to be used for analyzing scenarios.

Step 2: Characterize the Environment

- Identify core mission and business processes and key enterprise dependencies.
- Describe threat sources that are relevant to the enterprise. Include the motivation and resources available to the threat source, if applicable.
- List known vulnerabilities or areas of concern. (Note: 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.
- Define an acceptable level of risk (risk threshold) per the enterprise'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, enterprise changes, and new mission priorities.

Step 3: Develop and Select Threat Events for Analysis

- List possible ways that threat sources could exploit known vulnerabilities or impact areas of concern to create a list of events. (Note: Historical data is useful for determining 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 of the defined purpose and scope of the analysis.
- In more detail, describe the remaining potential threat events. Include the TTPs that a threat source may use to carry out attacks. (Note: The level of detail in the description is dependent on the needs of the enterprise.)
- 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 enterprise, 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 enterprise units and processes that would be affected, taking into account applicable regulations, standards, policies, and procedures; 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.
- Estimate the impact that these consequences would have on the mission and business processes, information, assets, enterprise units, and 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.)
- Identify those enterprise units, processes, information (access or flows), and/or assets that may or would be subsequently affected, as well as the consequences and impact levels until each affected critical item 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 that a new part is needed to bring the server back up, 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 standards or recommended controls can simplify this process. This appendix uses the controls in Appendix A of this document.
- 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, and time) to implement potential new or strengthened controls.
- 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: Consider the potential that one control will help mitigate the risk of 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.
- Evaluate the effectiveness of the Risk Exposure Framework, and make improvements as needed.

Table C-1: Sample Risk Exposure Framework

Threat Scenario	**Threat**	
	Threat Event Description	*Describe possible ways that 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 that a threat acting upon a vulnerability has on the confidentiality, integrity, and/or availability of the enterprise's operations, assets, and/or individuals.
Enterprise units, processes, information, assets, or stakeholders affected		*List the affected enterprise units, processes, information, assets, or stakeholders affected.*
Risk	**Impact**	*Enter an estimate of impact, loss, or harm that would result from the threat event materializing to affect the mission and business processes, information assets, or stakeholders. Estimates should preferably be provided in quantitative terms based on historical data and should take 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 enterprise operations, enterprise assets, individuals, other enterprises, 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 that a specific event or events may occur.* Likelihood: Chance of something happening
	Risk Exposure (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 enterprise'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 enterprise's operations, assets, or individuals that falls within the risk appetite and risk tolerance statements set by the enterprise.
Mitigation	**Potential Mitigating Strategies and C-SCRM Controls**	*List the potential mitigating risk strategies and any relevant C-SCRM controls.* C-SCRM Risk Mitigation: A systematic process for managing exposures to cybersecurity risk in supply chains, threats, and vulnerabilities throughout the supply chain and developing risk response strategies to the cybersecurity risks throughout the supply chain.
	Estimated Cost of Mitigating Strategies	*Enter the estimated cost of risk mitigation 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: The portion of risk that remains after security measures have been applied.

SAMPLE SCENARIOS

This appendix provides six 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 their 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 (i.e., High, Moderate, Low) for likelihood, impact, and risk, enterprises may use any number of different units of measure (e.g., CVSS score). Additionally, these scenarios vary slightly in their implementation of the risk response framework to show that the Risk Exposure Framework can be adapted as needed.

SCENARIO 1: Influence or Control by Foreign Governments Over Suppliers[40]

Background

An enterprise 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

Though sourcing from multiple vendors, ABC Company relies on suppliers in a single country (i.e., Southeast Asia). This exposes ABC Company to geopolitical threats due to the potential for policies of a single government to have a dramatic impact on the availability of supplied inputs.

Threat Event Description

The enterprise has established the following fictitious threat for the analysis exercise: Last year, new leadership took over the government of the country where ABC Company does most of their PCB business. This leadership has been focused on improving the financial and business environment within the country, allowing larger firms who set up headquarters and other major centers within the country advantages to do business more easily and cost-efficiently with suppliers within the same region. However, in February of 2019, the now-corrupt regime passed

[40] Scenario 1 prose is slightly modified (e.g., changed company names) from ICT SCRM Task Force: Threat Scenarios Report (v3), August 2021, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf. This report leveraged the 2015 version of NIST SP 800-161.

new legislation that established an additional 20 % 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, ABC Company's current inventory of PCBs was about 10 % 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 that the new tax law took effect, ABC Company had reached an inventory level of up to 15 % of yearly demand.

Outcome

Between February and June of 2019, ABC Company considered partnerships with new suppliers, but there were several issues identified. One in every 10 new suppliers that ABC Company contacted required a lead time for ramping up to the desired demand of anywhere from 6 months to 18 months. This would have necessitated additional work on ABC Company's part, including testing samples of the supplier PCBs, finalizing logistical details, and monitoring supplier-side activities, such as the procurement of raw materials and the acquisition of additional personnel and production space that were necessary to meet the new demand.

The second issue was that the current contracts with all five suppliers in Southeast Asia involved meeting minimum demand requirements, meaning that ABC Company was committed to purchasing a minimum of 100,000 PCBs per month for the duration of the contracts, which ranged anywhere from 3 months to 24 months in length. This would mean that 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 % cost increase, this eroded the margins of a PC from 13.5 % down to 4.5 % on average. For some of the lower-margin ABC Company offerings, it would likely result in discontinuing the line and using the more expensive PCBs on higher-end models that could carry more margin.

Enterprise Units and Processes Affected

N/A

Potential Mitigating Strategies and C-SCRM Controls

- Perform regular assessments and reviews of supplier risk.[41]
- Diversify suppliers by immediate location, as well as 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 an unexpected shortage of demand at critical times.

[41] The regular assessment and review of the supplier risk mitigating strategy was added to the original Scenario 1 text from the ICT SCRM Task Force: Threat Scenarios Report (v3), August 2021, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf. This report leveraged the 2015 version of NIST SP 800-161.

- Employ more resources in countries or regions of critical suppliers with the intent to source advanced notice of new legislation that may negatively affect business.

Table C-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 the 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 % 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 % 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 the higher demand. By June 1, the day the new tax law took effect, ABC Company had reached an inventory level up to 15 % of annual demand.
	Threat Event Outcome	ABC Company also considered partnering with new suppliers, but there were issues identified with this approach. 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. Additionally, current contracts with all five active suppliers in Southeast Asia stipulated minimum demand requirements, meaning that ABC Company was committed to purchasing a minimum of 100,000 PCBs per month for the duration of the contracts, which ranged anywhere from 3 months to 24 months in length. This would mean that ABC Company could not easily avoid the cost implications of the

		new tax. With a 20 % cost increase, the margins of a PC eroded from 13.5 % to 4.5 %, on average.	
Enterprise 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 Exposure (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	
Mitigation	**Potential Mitigating Strategies and C-SCRM Controls**	Assess and review supplier risk to include FOCI [SR-6(1)], employ supplier diversity requirements [C-SCRM_PL-3(1)], employ supplier diversity [SCRM_PL-8(2)], and adjust inventory levels [CM-8].	• Perform regular assessments and reviews of supplier risk. • Diversify suppliers by immediate location, as well as 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 it is the fault of the supplier or not). • Adjust desired inventory levels to better account for unexpected shortages of demand at critical times. • Employ more resources in countries or regions of critical suppliers with the intent to source advanced notice of new legislation 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 enterprise, 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 10 more years without any major upgrades or modifications and has a 99.9 % uptime requirement.
- Over 1,000 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 3-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 the 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 that restrict 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 the counterfeits, which are visually identical to their genuine counterparts but use lower-quality materials. The counterfeiters have the resources to copy most trademark and other identifying characteristics and insert counterfeits into a supply chain commonly used by the enterprise with little to no risk of detection. The

counterfeit product is appealing to unaware purchasing authorities as it is generally offered at a discount and sold as excess inventory or 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 randomly integrating with genuine parts in the system, the number and severity of unexpected outages could grow significantly. The agency and integrator decided that the chances that 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) who purchase the element from a supplier would be the first affected by a counterfeit product. Policy requires that 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 offered at a discount, there is a high chance that 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 to be replaced, an engineer will install a counterfeit, quickly test to ensure that it is running properly, and record the change. It could take two years for the counterfeit product to fail, and up to 200 counterfeit elements could be inserted into the system before the first sign of failure. If all of 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 10 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. Moreover, 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 Appendix A of 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].
- Employ supplier diversity requirements [PL-8(2)].

Based on these controls, the agency was able to devise a strategy that would include:

- Acceptance testing: The examination of elements to ensure that 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 in the design of the system by adding redundant elements along more critical paths (as determined by a criticality analysis) to minimize the impact of an element failure.
- 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 of implementing a more rigorous acquisition and testing program was $80,000. The cost of increasing security engineering requirements was $100,000.

Table C-3: Scenario 2

Threat Scenario	**Threat Source**	Counterfeit telecommunications element introduced into supply chain
	Vulnerability	Element no longer produced by OEM Purchasing authorities unable or unwilling to identify and purchase only genuine elements
	Threat Event Description	The threat agent inserts their counterfeit element into a trusted distribution chain. Purchasing authorities buy the counterfeit element. Counterfeit elements are installed into the system.
	Threat Event Outcome	The element fails more frequently than before, increasing the number of outages.
Enterprise units, processes, information, assets, or 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 the agency's inability to detect counterfeits with 25 % annualized probability of premature component failure

	Risk Exposure (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 and C-SCRM Controls**	Increase acceptance testing capabilities [C-SCRM_SA-9; C-SCRM_SA-10] and security requirements in the 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 enterprise 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 enterprise, ABC Company, and the integration company – to help identify the impacts that the partnership would have on the enterprise and risk-appropriate mitigation 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. The loss of availability of the element while the system is operational could have significant, immediate impacts across multiple agencies and the civilian populous, including the loss of life and millions of dollars in damages. An initial risk assessment was conducted using [NIST SP 800-30, Rev. 1], and the existing level of risk for this 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 and include the ability to provide both concessions and incentives to help KXY meet those requirements. The key area of concern is 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 the current mitigation strategies in place and determined that ABC Company, the integration company, and the enterprise 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 to be 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 be uniquely tagged using RFID technology or otherwise identified for traceability (Ref. SR-4).

Threat Scenario

Based on past experience, the enterprise decided that KXY's host nation would likely perform one of two actions if given access to the technology: 1) sell it to interested parties or 2) insert or 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 accomplished with the 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 include radiographic examination, material analysis, electrical testing, and sample accelerated life testing. Modifications to identification labels or 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 an approximately 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 exposure for the vulnerability of concern was "High."

Mitigating Strategies

Using Appendix A of 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 with suppliers. Require that the information be secured [Ref. AC-21].
- Require that 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 to the existing risk without the partnership at a cost increase that is less than if the enterprise had changed suppliers.

Table C-4: Scenario 3

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, and 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

<table>
<tr><td></td><td>Threat Event Outcome</td><td colspan="3">Nation-state extracts technology threat actor, modifies technology, or exploits previously unknown vulnerability</td></tr>
<tr><td colspan="2">Enterprise units, processes, information, assets, or stakeholders affected</td><td colspan="3">KXY Supplier
ABC Company integrator functionality testing
Technology users
Other federal agencies / customers</td></tr>
<tr><td rowspan="4">Risk</td><td>Impact</td><td colspan="2">Technology modified / vulnerabilities exploited – High</td><td>Technology sold to interested parties – Moderate</td></tr>
<tr><td>Likelihood</td><td colspan="2">Moderate</td><td>Moderate</td></tr>
<tr><td>Risk exposure (Impact x Likelihood)</td><td colspan="3">High</td></tr>
<tr><td>Acceptable Level of Risk</td><td colspan="3">Moderate</td></tr>
<tr><td rowspan="5">Mitigation</td><td>Potential Mitigating Strategies and C-SCRM Controls</td><td>(1) Improve traceability and monitoring capabilities</td><td>(2) Increase provenance and information control requirements</td><td>(3) Choose another supplier</td></tr>
<tr><td>Estimated Cost of Mitigating Strategies</td><td>20 % increase</td><td>20 % increase</td><td>40 % increase</td></tr>
<tr><td>Change in Likelihood</td><td colspan="3">Moderate → Low</td></tr>
<tr><td>Change in Impact</td><td colspan="3">High → Moderate</td></tr>
<tr><td>Selected Strategies</td><td colspan="3">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].</td></tr>
</table>

	Estimated Residual Risk	Moderate – The residual risk was determined to be equivalent to the existing risk without the partnership.

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 that run 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 the 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 trace 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 conducted 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, as well as 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 assume that there was a bug in the system. However, because the malicious code would be buried and difficult to identify, the integration company would not 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 (e.g., manual peer-review) [AC-1, AC-2, CM-3].
- Require static code testing [RA-9].
- Establish incident handling procedures [IR-4].

Table C-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	A 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.
Enterprise units, processes, information, assets, or 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 exposure (Impact x Likelihood)	High
	Acceptable Level of Risk	Moderate
Mitigation	**Potential Mitigating Strategies and 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 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 that 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 the 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 balancers and routers in the system design to save costs.

Threat Scenario Analysis

ABC Company decides that there are 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, and 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 are 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 the addition of configuration management controls that require that 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.

Table C-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, and routers are installed and start to fail, causing denial of service.
Enterprise units, processes, information, assets, or stakeholders affected.		None	Acquisitions	Acquisitions, System, Users
Risk	**Impact**	None	Low	High
	Likelihood	Moderate: 30 %	High: 40 %	Moderate: 30 %
	Risk Exposure (Impact x Likelihood)	None	Moderate	Moderate
	Acceptable Level of Risk	Low	Moderate	High
Mitigation	**Potential Mitigating Strategies and SCRM Controls**	Improve training program, and require that changes be approved by CMB.	Improve acquisition testing.	Improve the design of the 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 Exposure	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

SCENARIO 6: Vulnerable Reused Components Within Systems

Background

As part of their standard development practices, ABC Company reuses internally developed and open source system components in the development of their COTS solutions. Recent high-profile cyber attacks have capitalized on vulnerabilities present in reused system components, and ABC Company's customers are demanding increased transparency as a means of mitigating their own risk exposure.

ABC Company has decided to perform a threat scenario analysis to determine which steps can be taken to improve the security of their software products and offer customers greater confidence that ABC Company is taking the necessary steps to protect them from these types of attacks.

Environment

ABC Company is a well-known market-leader in the financial planning and analysis (FP&A) software market. ABC Company's customers rely on Acme's FP&A solution to store, process, and analyze sensitive financial information (e.g., closing the books).

Threat Event

Apache Struts (a widely-used software component) is used as a component within ABC Company's COTS FP&A solution. A vulnerability present in Apache Struts was patched in March of 2021. Motivated by financial gain, opportunistic cyber-criminal organizations sought opportunities to capitalize on vulnerabilities in COTS solutions.

ABC Company provides frequent updates to mitigate software vulnerabilities in their COTS solutions. However, in this case, the software component in question was not included as part of these updates.

The vulnerability in question is present and exploitable within ABC Company's FP&A solution.

Threat Scenario Analysis

If the attackers were to discover the vulnerability in ABC Company's product, a potential course of events could occur as follows:

> A well-resourced cyber-criminal organization could install rogue code in customer instances of the FP&A solution. Using this rogue code, the cyber criminals could extract and sell the sensitive, undisclosed financial information of public companies that trade on global stock markets. Upon discovery of the attack, ABC Company could face significant reputational harm due to the negative publicity. ABC Company's customers may engage in legal action against ABC Company as a result of their failure to appropriately patch known vulnerabilities in their software products.

Mitigating Strategies

ABC Company identified the following areas for improvement in order to enhance their secure software development practices and improve the confidence in their products:

- Ensure that developers receive training on secure development practices and are instructed on the use of vulnerability tooling so that developed software is secure.
- Ensure that reused system components – whether developed internally or open source – are evaluated as part of a standard process for known vulnerabilities (Ref. SA-15).
- Maintain a system component inventory to aid in maintenance of the software product throughout its life cycle (Ref. CM-8).
- Continuously monitor system components for vulnerabilities that arise, and ensure that appropriate processes are in place for expeditious remediation once a fix is available. Automate this process where possible (Ref. CA-7, RA-5).

Table C-7: Scenario 6

Threat Scenario	**Threat Source**	Cyber Criminal Organization – Vulnerable Software Components
	Vulnerability	Failure to understand and monitor the vulnerability state of reused components used in FP&A software products and provide timely updates to patch known vulnerabilities
	Threat Event Description	A cyber criminal organization exploits a known vulnerability in an FP&A software product to install rogue code and gain access to sensitive financial information contained within the application instances used by ABC Company customers.
	Existing Practices	ABC Company has a comprehensive and secure SDLC that focuses on identifying and mitigating vulnerabilities within their in-house developed code. ABC Company releases frequent patches to close vulnerabilities in their products.
	Threat Event Outcome	More than 10 major ABC Company customers are compromised as a result of the vulnerable software. Negative press surrounding the attack has led to significant impact (i.e., 5 % drop) to ABC Company's share price. ABC Company's competitors are capitalizing on the attack and using their own security practices to differentiate themselves and gain market share. ABC Company faces significant legal costs due to action taken by affected customers. ABC Company has seen a 5 % abnormal customer churn in the year following the attack.

Enterprise units, processes, information, assets, or stakeholders affected		FP&A Software Products Division
Risk	**Impact**	High – $350 million in aggregate cost, substantial reputational impact, and loss of market share, share price, and customers
	Likelihood	High – 20 % annual probability of occurrence
	Risk exposure (Impact x Likelihood)	High: $70 million loss exposure
	Acceptable Level of Risk	Moderate – $20 million: ABC Company's Risk Committee has stated that it is unwilling to lose more than $20 million due to a single cybersecurity event affecting customer products.
Mitigation	**Potential Mitigating Strategies and SCRM Controls**	• Ensure that developers receive training on secure development practices and are instructed on the use of vulnerability tooling so that developed software is secure. • Ensure that reused system components – whether developed internally or open source) are evaluated as part of a standard process for known vulnerabilities (Ref. SA-15). • Maintain a system component inventor to aid in the maintenance of the software product throughout its life cycle (Ref. CM-8). • Continuously monitor system components for vulnerabilities that arise, and ensure that appropriate processes are in place for expeditious remediation once a fix is available. Automate this process where possible (Ref. CA-7, RA-5).
	Estimated Cost of Mitigating Strategies	• Developer training: $500-$800K • System Component Inventory Process: $1.2-1.5 million • Continuous Monitoring of System Component Vulnerabilities: $800K – $1.2 million

	Change in Impact	High $350 million (no change based on identified controls)
	Change in Likelihood	Low 5 % annual probability of occurrence
	New Risk Exposure	Moderate: $17.5 million

APPENDIX D: C-SCRM TEMPLATES[42]

1. C-SCRM STRATEGY AND IMPLEMENTATION PLAN

To address cybersecurity risks throughout the supply chain, enterprises develop a C-SCRM strategy. The C-SCRM strategy, accompanied by an implementation plan, is at the enterprise level (Level 1), though different mission and business areas (Level 2) may further tailor the C-SCRM strategy to address specific mission and business needs, as outlined at the enterprise 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 enterprise's supply chain risk exposure via enterprise-wide risk management requirements, ownership, risk tolerance, roles and responsibilities, and escalation criteria. Note that the strategy and implementation plan may be developed as a single document or split apart into multiple documents. In any case, these C-SCRM outputs should be closely related in nature.

1.1. C-SCRM Strategy and Implementation Plan Template

1.1.1. Purpose

Outline the enterprise's high-level purpose for the strategy and implementation document, aligning that purpose with the enterprise's mission, vision, and values. Describe where the strategy and implementation document reside relative to other C-SCRM documentation that must be maintained at various tiers. Provide clear direction around the enterprise'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 enterprise in support of its vision, mission, and values.

The strategic approach is organized around a set of objectives that span the scope of the enterprise's mission and reflect a phased, achievable, strategic approach to ensuring the successful implementation and effectiveness of C-SCRM efforts across the enterprise.

This strategy and implementation document discusses the necessary core functions, roles, responsibilities, and the approach that the enterprise will take to implement C-SCRM capabilities within the enterprise. As mission and 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.

[42] Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

The focus of this strategy and implementation plan is intentionally targeted at establishing a core foundational capability. These baseline functions – such as defining policies, ownership, and dedicated resources – will ensure that the enterprise can expand and mature its C-SCRM capabilities over time. This plan also acknowledges and emphasizes the need to raise awareness among staff and ensure proper training 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 dependencies on industry-wide coordination efforts, processes, and decisions. As government and industry-wide direction, process guidance, and requirements are clarified and communicated, the enterprise will update and refine its strategy and operational implementation plans and actions.

1.1.2. Authority and Compliance

List 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
  - Executive Order 14028 of May 12, 2021, Improving the Nation's Cybersecurity
- 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 enterprise's stated purpose in pursuing sound C-SCRM practices and risk-reducing outcomes. Together, the objectives provide the enterprise with the essential elements needed to bring C-SCRM capabilities to life, and effectively pursue the enterprise'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 enterprise governance structure that integrates C-SCRM requirements and incorporates these requirements into enterprise policies
- Defining a supplier risk assessment approach
- Implementing a quality and reliability program that includes quality assurance and quality control processes 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 the proper implementation of policy, guidance, and controls
- Implementing a robust incident management program to successfully identify, respond to, and mitigate security incidents
- Including critical suppliers in contingency planning, incident response, and disaster recovery planning and testing

Sample Text

Objective 1: Effectively manage cybersecurity risks throughout the supply chain

This objective addresses the primary intent of the enterprise's pursuit of C-SCRM. Establishing and sustaining an enterprise-wide C-SCRM program will enable the enterprise's risk owners to identify, assess, and mitigate supply chain risk to the enterprise's assets, functions, and associated services. Implementing an initial capability that can sustain and grow in scope of focus, breadth, and depth of function will be done in phases and will incorporate holistic "people, process, and technology" needs to ensure that the enterprise 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 enterprise'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 to the enterprise's customers. This objective can be achieved by:

- Strengthening vetting processes, C-SCRM requirements, and oversight of external providers and
- Ensuring that customer needs are met in line with their cybersecurity risk appetite, tolerance, and environment.

Objective 3: Position the enterprise as an industry leader in C-SCRM

The enterprise is well-positioned to enable and drive forward improvements that address how cybersecurity risk is managed in supply chains across the industry. Therefore, the enterprise must use this position to advocate for communication, incentivization, and the education of industry players about the enterprise's requirements and expectations related to addressing supply chain risk.

1.1.4. Implementation Plan and Progress Tracking

Outline the methodology and milestones by which the progress of the enterprise's C-SCRM strategic objectives will be tracked. Though enterprise context heavily informs this process, enterprises should define prioritized time horizons to encourage the execution of tasks that are critical or foundational in nature. A common nomenclature for defining such time horizons is "crawl, walk, run" Regardless of the designated time horizon, the implementation of practical, prioritized plans is essential to building momentum in the establishment or enhancing C-SCRM capabilities.

Once the implementation plan is baselined, an issue escalation process and feedback mechanism are included to drive change to the implementation plan and progress tracking.

Sample Text

[The enterprise's] execution of its C-SCRM strategic objectives and the sustained operational effectiveness of underlying activities require a formal approach and commitment to progress tracking. [The enterprise] will track and assess implementation of its strategic objectives by defining subsidiary milestones and implementation dates in an implementation plan. Monitoring and reporting on elements of the implementation plan require shared responsibilities across multiple disciplines and a cross-enterprise, team-based approach.

The following implementation plan will be continuously maintained by mission and business owners and reviewed by the senior leadership team as a part of regular oversight activities. Risks and issues that impact the implementation plan should be proactively raised to senior leadership team by mission and business owners or their team. The implementation plan may then be revised in accordance with the senior leadership's discretion.

Table D-1: Objective 1 – Implementation milestones to effectively manage cybersecurity risks throughout the supply chain

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 the enterprise risk management (ERM) framework	Delayed	…	Do Later	…

Implementation Plan Milestone	Status	Owner	Priority	Target Date
Establish a C-SCRM PMO capability	Cancelled	…	…	…
Establish roles and responsibilities, and assign accountability	…	…	…	…
Develop C-SCRM plans	…	…	…	…
Establish the 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	…	…	…	…

Table D-2: Objective 2 – Implementation milestones for serving 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 that customer support personnel are well-versed in management requirements and cybersecurity risks throughout the supply chain	Complete	…	Do Next	…
Establish minimum baseline levels of cybersecurity supply chain assurance	Delayed	…	Do Later	…
Establish processes to respond to identified risks and to monitor for impacts to the enterprise's supply chain	Cancelled	…	…	…

Table D-3: Objective 3 – Implementation milestones to position the enterprise 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 and shared services	Complete	…	Do Next	…
Advocate for C-SCRM awareness and competency through training and workforce development, to include secure coding training for developers	Delayed	…	Do Later	…
Release white papers and public guidance related to C-SCRM	Cancelled	…	…	…

1.1.5. Roles and Responsibilities

Designate those responsible for the Strategy and 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., enterprise affiliation, address, email address, and phone number).

Sample Text

- Senior leadership 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 enterprise's risk posture in a timely manner.

- Mission and business owners shall:
    - Determine mission-level risk appetite and tolerance, ensuring that they are in line with enterprise expectations;
    - Define supply chain risk management requirements and the implementation of controls that support enterprise objectives;
    - Maintain criticality analyses of mission functions and assets; and

- Perform risk assessments for mission and business-related procurements.

1.1.6. Definitions

List the key definitions described within the Strategy and Implementation template, and provide enterprise-specific context and examples where needed.

Sample Text

- Enterprise: An organization with a defined mission, goal, and boundary that uses information systems to execute that mission and has the 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 enterprise's broad expression of goals and a specified target outcome for operations.

1.1.7. Revision and Maintenance

Define the required frequency of Strategy and Implementation template revisions. Maintain a table of revisions to enforce version control. Strategy and Implementation templates are living documents that must be updated and communicated to all appropriate individuals (e.g., staff, contractors, and suppliers).

Sample Text

[The enterprise's] Strategy and Implementation template must be reviewed every 3-5 years (within the federal environment), at a minimum, 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 and Implementation template,
- Significant Strategy and Implementation events,
- The introduction of new technologies,
- The discovery of new vulnerabilities,
- Operational or environmental changes,
- Shortcomings in the Strategy and Implementation template,
- Change of scope, and
- Other enterprise-specific criteria.

Table D-4: Version Management Table

Version Number	Date	Description of Change/Revision	Section/Pages Affected	Changes made by Name/Title/Enterprise

2. C-SCRM POLICY

The C-SCRM policies direct the implementation of the C-SCRM strategy. The C-SCRM policies can be developed at Level 1 and/or at Level 2 and are informed by mission- and business-specific factors, including risk context, risk decisions, and risk activities from the C-SCRM strategy. The C-SCRM policies support applicable enterprise 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 enterprise's C-SCRM strategy, which in turn is informed by the enterprise's strategic plan. The C-SCRM policies should also address mission and business functions, as well as internal and external customer requirements. C-SCRM policies also define the integration points for C-SCRM with the risk management processes for the enterprise. Finally, the C-SCRM policies the C-SCRM roles and responsibilities within the enterprise define at a more specific and granular level, any interdependencies among those roles, and the interaction between the roles. The C-SCRM policies at Level 1 are broader, whereas the C-SCRM policies at Level 2 are specific to the mission and business function. C-SCRM roles specify the responsibilities for procurement, conducting risk assessments, collecting supply chain threat intelligence, identifying and implementing risk-based mitigations, monitoring, and other C-SCRM functions.

2.1. C-SCRM Policy Template

2.1.1. Authority and Compliance

List the laws, executive orders, directives, regulations, policies, standards, and guidelines that govern the C-SCRM policy.

Sample Level 1 Text

- Policies
  - [Enterprise Name] Enterprise Risk Management Policy
  - [Enterprise 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
  - [Enterprise Name] C-SCRM Policy
  - [Mission and Business Process Name] Information Security Policy

- Regulations
  - NYDFS 23 NYCRR 500: Section 500.11 Third-Party Service Provider Security Policy
- Guidelines
  - NIST 800-53, Revision 5: SR-1, PM-9, PM-30, PS-8, SI-12
  - NIST 800-161, Revision 1: Appendix C

2.1.2. Description

Describe the purpose and scope of the C-SCRM policy, outline the enterprise leadership's intent to adhere to the plan, enforce its controls, and ensure that it remains current. Define the tier(s) at which the policy applies. C-SCRM policies may need to be derived in whole or in part from existing policies or other guidance.

For Level 2, C-SCRM policies should list all Level 1 policies and plans that inform the Level 2 policies, provide a brief explanation of what the mission and business encompass, and briefly describe the scope of applicability (e.g., plans, systems, type of procurements, etc.) for the Level 2 C-SCRM policies.

Sample Level 1 Text

[The enterprise] is concerned about the risks in the products, services, and solutions bought, used, and offered to customers.

The policy objective of the [the enterprise's] C-SCRM Program is to successfully implement and sustain the capability of providing improved assurance that the products, services, and solutions used and offered by [the enterprise] are trustworthy, appropriately secure and resilient, and able to perform to the required quality standard.

C-SCRM is a systematic process for identifying and assessing susceptibilities, vulnerabilities, and threats throughout the supply chain and implementing strategies and mitigation controls to reduce risk exposure and combat threats. The establishment and sustainment of an enterprise-wide C-SCRM Program will enable [the enterprise's] risk owners to identify, assess, and mitigate supply chain risk to [the enterprise's] mission assets, functions, and associated services.

Sample Level 2 Text

[The mission and business process] recognizes its criticality to [the enterprise's objectives]. A key component of producing products involves coordinating among multiple suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. [The mission and business process] recognizes that the realization of cybersecurity risks throughout the supply chain may disrupt or completely inhibit [the mission and business process's] ability to generate products in a timely manner and in accordance with the required quality standard.

Based on the C-SCRM objectives set forth by [Enterprise Level 1 Policy], [the mission and business process's] policy objective is to implement C-SCRM capabilities that allow for the

assessment, response, and monitoring of cybersecurity risks throughout the supply chain. 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 [the mission and business process] 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 enterprise's C-SCRM strategic plan, mission and business functions, and internal and external customer requirements.

Sample Level 1 Text

[The enterprise's] enterprise-level C-SCRM Program is established to implement and sustain the capability to:

- Assess and provide appropriate risk response to cybersecurity risks that arise from the acquisition and use of covered articles;
- Prioritize assessments of cybersecurity risks throughout the supply chain and risk response actions based on criticality assessments of the mission, system, component, service, or asset;
- Develop an overall C-SCRM strategy and high-level implementation plan, 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 designated senior leadership who shall function as [the enterprise's] C-SCRM Program Executive and chair the C-SCRM Program Management Office (PMO);
- Leverage and be appropriately integrated into [the enterprise's] existing risk management and decision-making governance processes and structures;
- Reflect a team-based approach and be collaborative, interdisciplinary, and intra-enterprise in nature and composition;
- Incorporate a Level risk management approach that is consistent with the NIST Risk Management Framework and NIST SP 800-161, Rev. 1; and
- Implement codified and regulatory C-SCRM requirements and industry-wide and enterprise-specific policy direction, guidance, and processes.

Sample Level 2 Text

[The mission and business process's] C-SCRM Program shall:

- Operate in accordance with the requirements and guidance set forth by [the enterprise's] C-SCRM Program;
- Collaborate with the C-SCRM Program Management Office (PMO) to apply the C-SCRM practices and capabilities needed to assess, respond to, and monitor cybersecurity risks arising from pursuit of [the mission and business process's] core objectives;
- Integrate C-SCRM activities into applicable activities to support [the enterprise's] objective to manage cybersecurity risks throughout the supply chain;
- Assign and dedicate the resources needed for coordinating C-SCRM activities within [the mission and business process];
- Identify [the mission and business process's] critical suppliers, and assess the level of risk exposure that arises from that relationship;
- Implement risk response efforts to reduce exposure to cybersecurity risks throughout the supply chain; and
- Monitor [the mission and business process's] ongoing cybersecurity risk exposure in the supply chain profile, and provide periodic reporting to identified enterprise risk management and C-SCRM stakeholders.

2.1.4. Roles and 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., enterprise 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, implementation plans, and actions that address C-SCRM-related issues; program reporting and oversight; and identifying and making program resource recommendations.
    - Escalating and/or reporting C-SCRM issues to Senior Officials, as may be appropriate.

- Each C-SCRM Security Officer shall be responsible for:
    - Identifying C-SCRM Leads (the Lead will be responsible for participating as a collaborative and core member of the C-SCRM PMO);
    - Incorporating relevant C-SCRM functions into enterprise and position-level functions; and
    - Implementing and conforming to C-SCRM Program requirements.

Sample Level 2 Text

- C-SCRM Leads shall be responsible for:
    - Representing the interests and needs of C-SCRM PMO members.
    - Leading and/or coordinating the development and execution of program or business-line C-SCRM plans. This shall include ensuring that such plans are appropriately aligned to and integrated with the enterprise-level C-SCRM plan.

- The mission and business process C-SCRM staff shall be responsible for:
    - The primary execution of C-SCRM activities (e.g., supplier or product assessments) and
    - Support for mission- and business-specific C-SCRM activities driven by non-C-SCRM staff.

2.1.5. Definitions

List the key definitions described within the policy, and provide enterprise-specific context and examples where needed.

Sample Text (Applies to Level 1 and/or Level 2)

- Covered Articles: Information technology, including cloud computing services of all types; telecommunications equipment or telecommunications services; the processing of information on a federal or non-federal information system, subject to the requirements of the Controlled Unclassified Information program; and all IoT/OT (e.g., hardware, systems, devices, software, or services that include embedded or incidental information technology).
- Cybersecurity Supply Chain Risk Assessment: A systematic examination of cybersecurity risks throughout the supply chain, the likelihoods of their occurrence, and potential impacts.
- Risk Owner: A person or entity with the accountability and authority to manage a risk.

2.1.6. Revision and Maintenance

Define the required frequency for revising and maintaining the C-SCRM policy. Maintain a table of revisions to enforce version control. C-SCRM policies are living documents that must be updated and communicated to all appropriate individuals (e.g., staff, contractors, and suppliers).

Sample Text (Applies to Level 1 and/or Level 2)

[The enterprise's] C-SCRM policy must be reviewed on an annual basis, at minimum, since changes to laws, policies, standards, guidelines, and controls are dynamic and evolving. Additional criteria that may trigger interim revisions include:

- A change of policies that impact the C-SCRM policy,
- Significant C-SCRM events,

- The introduction of new technologies,
- The discovery of new vulnerabilities,
- Operational or environmental changes,
- Shortcomings in the C-SCRM policy,
- A change of scope, and
- Other enterprise-specific criteria.

Table D-5: Version Management Table

Version Number	Date	Description of Change/Revision	Section/Pages Affected	Changes made by Name/Title/Enterprise

3. C-SCRM PLAN

The C-SCRM plan is developed at Tier 3, is implementation-specific, and provides policy implementation, requirements, constraints, and implications. It can either be stand-alone or a component of a system security and privacy plan. If incorporated, the C-SCRM components must be clearly discernable. The C-SCRM plan addresses the management, implementation, and monitoring of C-SCRM controls and the development and 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 that supply chains can differ significantly across and within enterprises, C-SCRM plans should be tailored to individual programs, enterprises, 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 enterprises 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. Enterprises have the flexibility to develop and implement various approaches for the development and presentation of the C-SCRM plan. Enterprises can leverage automated tools to ensure that 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 and 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 supply chain cybersecurity controls in place or planned for implementation to provide fit-for-purpose C-SCRM controls that are 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 enterprise'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 that the C-SCRM plan describes the system in the context of the enterprise'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 and business functions of the system; the authorization boundary of the system; the overall system architecture, including any supporting systems and relationships; how the system supports enterprise missions; and the system environment (e.g., stand-alone, managed/enterprise, custom/specialized, security-limited functionality, cloud) established in Level 1 and Level 2.

Sample Text

[The enterprise'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, [supplier's name], within the United States. It has been functionally configured to meet the enterprise's needs. No third-party code libraries are utilized to deploy or maintain the system. It is hosted within the management layer of the enterprise's primary virtual private cloud provider.

The DMS is a Category 1 system that mandates a recovery time objective (RTO) of 1 hour in the event of downtime. The enterprise maintains a disaster recovery environment with a second private cloud provider to which the enterprise can switch if the Category 1 RTO is not likely to be met on the primary platform.

3.1.3. System Information Type and Categorization

The following tables specify the information types that are processed, stored, or transmitted by the system and/or its in-boundary supply chain. Enterprises utilize [NIST SP 800-60 v2], [NARA CUI], or other enterprise-specific information types to identify information types and provisional impact levels. Using guidance regarding the categorization of federal information and systems in [FIPS 199], the enterprise determines the security impact levels for each information type. Articulate the impact level (i.e., low, moderate, high) for each security objective (i.e., confidentiality, integrity, availability).

Sample Text

Table D-6: System Information Type and Categorization

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.

Table D-7: Security Impact 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

Table D-8: System Operational Status

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, and Life Cycle Activities

Include a current and detailed system and network diagram with 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 that activities are mapped and tracked. This guarantees full coverage of C-SCRM activities since these activities may require repeating and reintegrating (using spiral or agile techniques) throughout the life cycle. 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 and 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, the date of the agreement, the security authorization status of the other systems, the name of the authorizing official, a description of the connection, and diagrams that show the flow of any information exchange.

Sample Text

Table D-9: Information Exchange and System Connections

Agreement Date	Name of System	Enterprise	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 that the plan addresses requirements for developing trustworthy, secure, privacy-protective, and resilient system components and systems, including the application of 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, products, services, 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 enterprise established a C-SCRM program to address the management of cybersecurity risks throughout the supply chain. The C-SCRM PMO is responsible for conducting assessments of cybersecurity risks that arise from 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: The 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 preparation 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 alternative phone number, and email address of key cybersecurity supply chain personnel or designate contacts (e.g., vendor contacts, acquisitions subject matter experts [SME], engineering leads, business partners, service providers) with a role, name, address, primary and alternative phone numbers, and email address.

Sample Text

Table D-10: Role Identification

Role	Name	Department/ Division	Primary Phone Number	Alternative Phone Number	Email Address
Vendor Contact					
Acquisitions SME					
Engineering Lead					
Business Partner					
Service Provider					

3.1.9. Contingencies and Emergencies

For organizations that choose to acquires products in the event of contingency or emergency operations, enterprises may need to bypass normal C-SCRM acquisition processes to allow for mission continuity. Contracting activities that are not vetted using approved C-SCRM plan processes introduce operational risks to the enterprise.

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 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, and Policies

List any applicable laws, executive orders, directives, policies, and regulations that are applicable to the system (e.g., Executive Order 14028, FAR, FERC, etc.). For Level 3, include applicable Level 1 C-SCRM Strategy and Implementation Plans and Level 2 C-SCRM Policy titles.

Sample Text

The enterprise shall ensure that C-SCRM plan controls are consistent with applicable statutory authority, including the Federal Information Security Modernization Act (FISMA); 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 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, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-161, Rev. 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*
- OMB Circular A-130 *Managing Information as a Strategic Resource*
- Federal Acquisition Supply Chain Security Act of 2018
- Executive Order 14028 of May 12, 2021, *Improving the Nation's Cybersecurity*

3.1.11. Revision and Maintenance

Include a table that identifies 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 them for compliance with upper tier plans as appropriate. Ensure that the plan adapts to the shifting impacts of exogenous factors, such as threats and changes to the enterprise or environmental.

Sample Text

Table D-11: Revision and Maintenance

Version Number	Date	Description of Change/Revision	Section/Pages Affected	Changes made by Name/Title/Enterprise

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

Table D-12: Acronym List

Acronym	Detail
AO	Authorizing Official
C-SCRM	Cybersecurity 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
- C-SCRM plans of contractors or suppliers

3.1.15. C-SCRM Plan and Life Cycles

C-SCRM plans should cover the full SDLC of systems and programs, including research and development, design, manufacturing, acquisition, delivery, integration, operations, and disposal/retirement. The C-SCRM plan activities should be integrated into the enterprise's system and software life cycle processes. Similar controls in the C-SCRM plan can be applied in more than one life cycle process. The figure below shows how the C-SCRM plan activities can be integrated into various example life cycles.

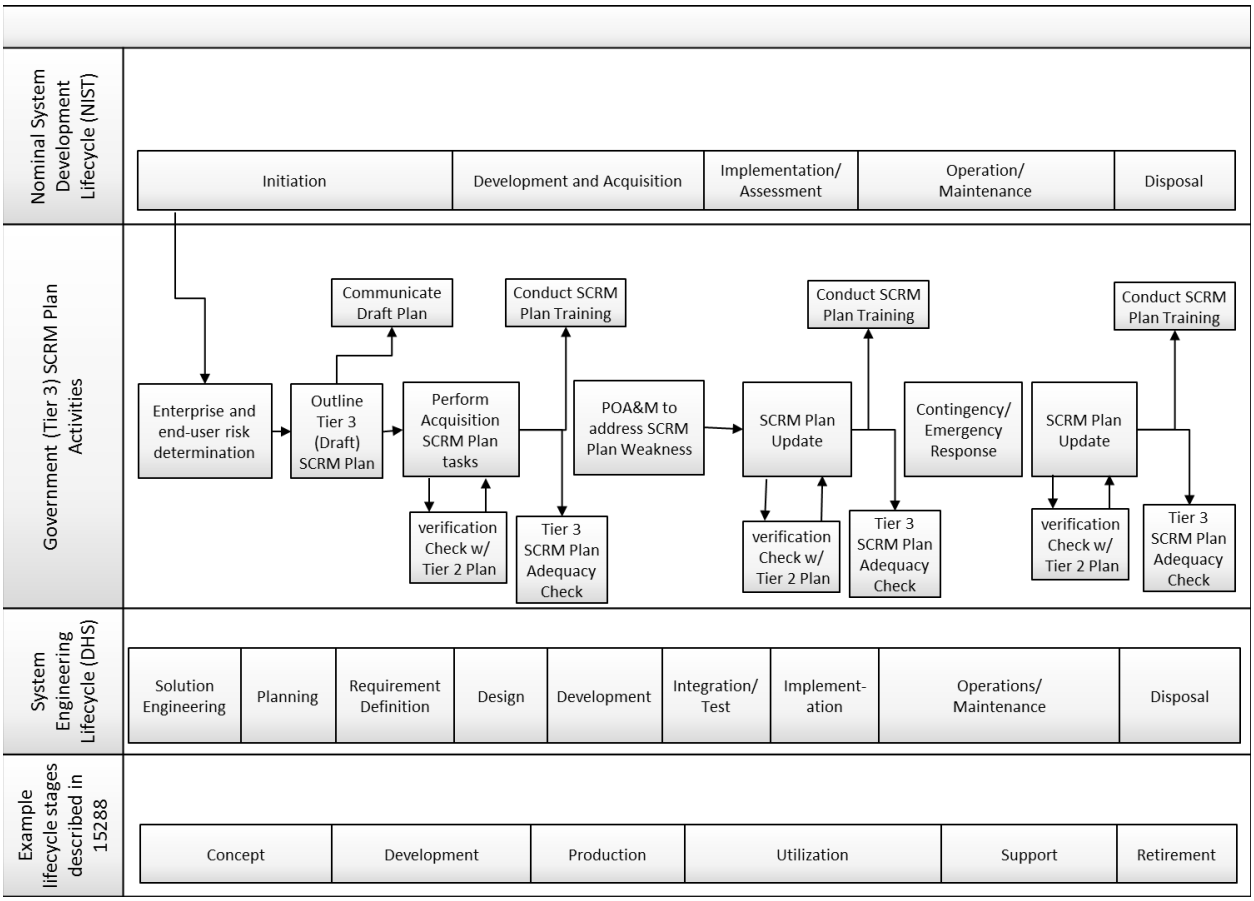

Fig. D-1: Example C-SCRM Plan Life Cycle

4. CYBERSECURITY SUPPLY CHAIN RISK ASSESSMENT TEMPLATE

The Cybersecurity Supply Chain Risk Assessment (C-SCRA)[43] guides the review of any third-party product, service, or supplier[44] that could present a cybersecurity 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-SCRAC-SCRA considers available public and private information to perform a holistic assessment, including known cybersecurity risks throughout the supply chain, the likelihoods of their occurrence, and their potential impacts on an enterprise and its information and systems. As enterprises may be inundated with C-SCRAC-SCRAs and suppliers inundated with C-SCRAC-SCRA requests, the enterprise should evaluate the relative priority of its C-SCRAC-SCRAs as an influencing factor on the rigor of the C-SCRAC-SCRA.

As with the other featured templates, the below C-SCRAC-SCRA is provided only as an example. Enterprises must tailor the below content to align with their Level 1 and Level 2 risk postures. The execution of C-SCRAC-SCRA 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. Federal agencies should refer to Appendix E for additional guidance concerning supply chain risk assessments.

4.1. C-SCRM Template

4.1.1. Authority and Compliance

List the laws, executive orders, directives, regulations, policies, standards, and guidelines that govern C-SCRAC-SCRA execution.

Sample Text

- Legislation
  - Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology of 2018
- Policies
  - [Enterprise name] C-SCRA Standard Operating Procedures
  - [Enterprise name] C-SCRA Risk Assessment Factors
  - [Enterprise name] C-SCRA Criticality Assessment Criteria
- Guidelines
  - NIST 800-53, Rev. 5: PM-30, RA-3, SA-15, SR-5
  - NIST 800-37, Rev. 2
  - NIST 800-161, Rev. 1: Appendix C
  - ISO 28001:2007

[43] For the purposes of this document, the expression "cybersecurity supply chain risk assessment" should be considered equivalent to "supply chain risk assessment" in an effort to harmonize terminology.
[44] 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, and reference the enterprise commitment to C-SCRM and mandate to perform C-SCRAs as an extension of that commitment. Outline the template's relationship to enterprise risk management principles, frameworks, and practices. This may include providing an overview of the enterprise's C-SCRA processes, standard operating procedures, and/or criticality designations that govern the usage of this template.

Reinforce the business case for executing C-SCRA by highlighting the benefits of reducing expected loss from adverse supply chain cybersecurity events, as well as the C-SCRM PMO's role in efficiently executing these assessments at scale.

Provide an overview of the enterprise's 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 fairly and consistently evaluate risks posed to the [enterprise] via third parties that hold the potential for harm or compromise as a result of cybersecurity risks. Cybersecurity risk in the supply chain 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 C-SCRM PMO to review cybersecurity risk in the supply chain and ensure that C-SCRAs are appropriately, efficiently, and effectively carried out in line with enterprise mandates.

Requestors seeking to introduce third-party products, services, or suppliers into enterprise 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 adherence to the steps of the C-SCRA.

The C-SCRA process contains five primary steps, as outlined in the below template:[45]

1. Information Gathering and Scoping Analysis
2. Threat Analysis
3. Vulnerability Analysis
4. Impact Analysis
5. Risk Response Analysis

[45] 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 [enterprise's intranet page] or contact [C-SCRM PMO email].

4.1.3. Information Gathering and Scoping Analysis

Define the purpose and objectives for the requested C-SCRA, and outline the key information required to appropriately define the system, operations, supporting architecture, and boundaries. Provide key questions to requestors to facilitate the 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

Table D-13: Information Gathering and Scoping Analysis

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 % of this supplier's sales of this product/service does your enterprise consume?		Acquirer or Supplier
How widely used is or will the product or service be in your enterprise?		Acquirer
Is the product/service manufactured in a geographic location that is considered an area of geopolitical risk for your enterprise based on its primary area of operation (e.g., in the United States)?		Acquirer or Supplier
Is the product manufactured or developed in a country identified as a foreign adversary or country of special concern?		Acquirer

Would switching to an alternative supplier for this product or service constitute significant cost or effort for your enterprise?		Acquirer
Does your enterprise have an existing relationship with another supplier for this product/service?		Acquirer
How confident is your enterprise that they will be able to obtain quality products/services regardless of major supply chain disruptions, both human and natural?		Acquirer
Does your enterprise maintain a reserve of this product/service?		Acquirer
Is the product/service fit for purpose? (i.e., capable of meeting objectives or service levels)?		Acquirer
Does the product/service perform an essential security function? If so, 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
In the event of compromise leading to system failure or severe degradation, is there a known independent reliable mitigation?		Acquirer
Will/does the product/service connect to a platform that is provided to customers by your enterprise?		Acquirer
Will/does the product/service transmit, generate, maintain, or process high value data (e.g., PII, PHI, PCI)?		Acquirer
Will/does the product/service have access to systems that transmit, generate, maintain or process high value data (e.g., PII, PHI, PCI)?		Acquirer

Will/does the supplier require physical access to the company's 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 enterprise (i.e., critical, high, moderate, low)?		Acquirer
Section 3: Supplier Overview		
Have you identified the supplier's critical suppliers?		Supplier
Did you verify the supplier ownership, whether foreign and domestic?		Supplier
If the supplier uses distributors, did you investigate them for potential risks?		Supplier
Is the supplier located in the United States?		Supplier
Does the supplier have personnel and/or professional ties (including its officers, directors, or similar officials, employees, consultants, or contractors) with any foreign government?		Supplier
Is there foreign ownership, control, or influence (FOCI) over the supplier or any business entities involved in the supply chain? If so, is the FOCI from a foreign adversary of the United States or country of concern?		Supplier
Do the laws and regulations of any foreign country in which the supplier has headquarters, research development, manufacturing, testing, packaging, distribution, or service facilities or other operations require the sharing of technology or data with that foreign country?		Supplier
Has the supplier declared where replacement components will be purchased from?		Supplier

Have the owners and locations of all of the suppliers, subcontractors, and sub-tier suppliers been identified and validated?		Supplier
Does the supplier employ the use of threat scenarios to inform the vetting of sub-tier suppliers?		Supplier
Does the supplier have documents that track part numbers to manufacturers?		Supplier
Can the supplier provide a list of who they procure hardware and software from that is utilized in the performance of the contract?		Supplier
Does the supplier have counterfeit controls in place?		Supplier
Does the supplier safeguard key program information that may be exposed through interactions with other suppliers?		Supplier
Does the supplier perform reviews and inspections and have safeguards to detect or avoid counterfeit equipment, tampered hardware or software (HW/SW), vulnerable HW/SW, and/or operations security leaks?		Supplier
Does the supplier use industry standard baselines (e.g., CIS, NES) when purchasing software?		Supplier
Does the supplier comply with regulatory and legislative mandates?		Supplier
Does the supplier have procedures for secure maintenance and upgrades following deployment?		Supplier
Section 4: Policies and 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 capabilities?		Supplier

Does everyone associated with the procurement (e.g., supplier, C-SCRM PMO) understand the potential threats to and risks in the subject supply chain?		Supplier
What is the citizenship of all engaged personnel? If required, 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 who 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 remotely access environments?		Supplier
Section 5: Logistics (if applicable)		
Does the supplier have documented tracking and version controls in place?		Supplier
Does the supplier analyze events (environmental or human-made) that could interrupt their supply chain?		Supplier
Are the supplier's completed parts controlled so that they are never left unattended or exposed to tampering?		Supplier
Are the supplier's completed parts locked up?		Supplier
Does the supplier have a process that ensures integrity when ordering inventory from their supplier?		Supplier
Is the supplier's inventory periodically inspected for exposure or tampering?		Supplier
Does the supplier have secure material destruction procedures for unused and scrap parts procured from their supplier?		Supplier

Is there a documented chain of custody for the deployment of products and systems?		Supplier
Section 6: Software Design and Development (if applicable)		
Is the supplier familiar with all of their 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 Life Cycle)?		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 7: Product- or Service-specific Security (if applicable, one questionnaire per product/service)		
Name of Product or Service		Manufacturer
Product Type (i.e., hardware, software, service)		Manufacturer
Description of Product or Service		Manufacturer
Part Number (if applicable)		Manufacturer

Does the manufacturer implement formal enterprise 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 that conform to standards such as ISO 27036 or SAE AS6171?		Manufacturer
Is the product compliant with Federal Information Processing Standards (FIPS) 140-2? 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 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, service, or components, including 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 in their product offerings or solutions?		Manufacturer
Does the manufacturer manage the integrity of IP for its products or service offerings?		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 to reduce 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 for ensuring that 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. Include a rubric with categorical definitions to encourage the transparency of 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 supply chain. Following completion of the analysis, one of the following threat levels is assigned:

- **Critical:** Information indicates that an adversarial or non-adversarial threat is imminent (e.g., an adversary is actively engaged in subversion, exploitation, or sabotage of the product, service, or supplier).
- **High:** Information indicates that an adversarial or non-adversarial threat is imminent (e.g., significant drought in the geographical area combined with location characteristics of the asset yields high potential for forest fires).

- **Moderate:** Information indicates that an adversarial or non-adversarial threat has an average potential to impact or target the enterprise (e.g., a specific adversarial threat exists but lacks either the capability or the intent to engage in subversion, exploitation or sabotage of the product, service, or supplier).
- **Low:** Information indicates that adversarial or non-adversarial threats are non-existent, unlikely, or have below average potential to impact or target the enterprise (e.g., adversarial threats lack both the capability and 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 and Scoping questionnaire to coordinate the 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 of the aforementioned topics should be performed if red flags are observed during initial data collection.

4.1.5. Vulnerability Analysis

Define vulnerability analysis and 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 life cycle 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 supply chain. Following completion of the analysis, one of the following threat levels is assigned:

- **Critical:** The product, service, or supplier contains vulnerabilities or weaknesses that are wholly exposed and easily exploitable.
- **High:** The product, service, or supplier contains vulnerabilities or weaknesses that are highly exposed and reasonably exploitable.
- **Moderate:** The product, service, or supplier contains vulnerabilities or weaknesses that are moderately exposed and difficult to exploit.
- **Low:** The product, service, or supplier contains vulnerabilities and weaknesses with limited exposure and are unlikely to be exploited.

To appropriately assign the above vulnerability analysis designation, C-SCRM PMOs and requestors should coordinate the collection of 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 and 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 the transparency of assessment results.

Sample Text

The C-SCRA impact analysis evaluates and then characterizes the impact of the product, service, or supplier throughout its life cycle 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 enterprise's operations or mission. Upon 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 enterprise 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 enterprise 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 enterprise failure that could be readily and quickly managed with no long-term consequences.
- **Low:** The product, service, or supplier's failure to perform as designed would result in few adverse effects on the enterprise, and those effects could be readily and quickly managed with no long-term consequences.

To appropriately assign the above impact analysis designation, C-SCRM PMOs and requestors should coordinate the collection of information related to the enterprise's critical functions and components, the identification of the intended user environment for the product or service, and supplier information.

4.1.7. Risk Response Analysis

Define risk analysis and 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 the transparency of assessment results.

Sample Text

The C-SCRA risk exposure 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
	Critical	Moderately Likely	Highly Likely	Very Likely	Very Likely
	High	Moderately Likely	Highly Likely	Highly Likely	Very Likely
	Moderate	Unlikely	Moderately Likely	Highly Likely	Highly Likely
	Low	Unlikely	Unlikely	Moderately Likely	Moderately Likely

Fig. D-2: Example Likelihood Determination

The C-SCRA risk exposure is then aggregated based on 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 on its likelihood and impact.

Overall Risk Exposure					
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

Fig. D-3: Example Risk Exposure Determination

The aforementioned risk analyses and scoring provide measures by which the enterprise determines whether or not to proceed with procurement of the product, service, or supplier. Decisions to proceed must be weighed against the risk appetite and tolerance across the tiers of the enterprise, 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 and 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., enterprise affiliation, address, email address, and phone number).

Sample Text

- The C-SCRM PMO shall:
    - Maintain C-SCRA policies, procedures, and scoring methodologies;
    - Perform C-SCRA standard operating procedures;
    - Liaise with requestors seeking to procure a product, service, or supplier; and
    - Report C-SCRA results to leadership to help inform enterprise 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, and
    - Adhere 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, and provide enterprise-specific context and examples where needed.

Sample Text

- Procurement: The process of obtaining a system, product, or service.

4.1.10. Revision and Maintenance

Define the required frequency for updating 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

The enterprise's C-SCRA template must be reviewed on an annual basis, at a minimum, since changes to laws, policies, standards, guidelines, and controls are dynamic and evolving. Additional criteria that may trigger interim revisions include:

- A change of policies that impact the C-SCRA template,
- Significant C-SCRM events,
- The introduction of new technologies,
- The discovery of new vulnerabilities,
- Operational or environmental changes,

- Shortcomings in the C-SCRA template,
- A change of scope, and
- Other enterprise-specific criteria.

Sample Text

Table D-14: Version Management Table

Version Number	Date	Description of Change/Revision	Section/Pages Affected	Changes made by Name/Title/Enterprise

APPENDIX E: FASCSA[46]

INTRODUCTION

Purpose, Audience, and Background

This Appendix augments the content in NIST SP 800-161, Rev. 1 and provides additional guidance specific to federal executive agencies related to supply chain risk assessment factors, assessment documentation, risk severity levels, and risk response.

As discussed in the introductory section of the main body of SP 800-161, Rev 1., *The Federal Acquisition Supply Chain Security Act of 2018* (FASCSA), Title II of the *SECURE Technology Act* (P. L. 115-390), was enacted to improve executive branch coordination, supply chain risk information (SCRI) sharing, and actions to address supply chain risks. The law established the Federal Acquisition Security Council (FASC),[47] an interagency executive body at the federal enterprise level. This council is authorized to perform a range of functions intended to reduce the Federal Government's supply chain risk exposure and risk impact.

The FASCSA provides the FASC and executive agencies with authorities relating to mitigating supply chain risks, to include the exclusion and/or removal of sources and covered articles.[48] The law also mandates that agencies conduct and prioritize supply chain risk assessments (SCRAs). The guidance in this appendix is specific to this FASCSA requirement, as described below, and addresses the need for a baseline level of consistency and alignment between agency-level C-SCRM risk assessment and response functions and those SCRM functions that occur at the government-wide level by authorized bodies such as the FASC.

Scope

IN SCOPE

This appendix is primarily focused on providing agencies with additional guidance concerning Section 1326 (a) (1) of the FASCSA,[49] which requires executive agencies to assess the supply chain risk posed by the acquisition and use of covered articles and to respond to that risk as appropriate. The law directs agencies to perform this activity and other SCRM activities described therein, consistent with NIST standards, guidelines, and practices.

OUT OF SCOPE

Section 4713 of the FASCSA[50] pertains to executive agencies' authority to carry out covered procurement actions. Specific guidance concerning those actions is outside of the scope of this

[46] Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.
[47] For additional information about the FASC authorities, membership, functions, and processes, readers should refer to the Federal Acquisition Security Council Final Rule, 41 CFR Parts 201 and 201-1. See: https://www.govinfo.gov/content/pkg/FR-2021-08-26/pdf/2021-17532.pdf.
[48] As defined by FASCSA, a covered article means: Information technology, including cloud computing services of all types; telecommunications equipment or telecommunications services; the processing of information on a federal or non-federal information system, subject to the requirements of the Controlled Unclassified Information program; all IoT/OT (e.g., hardware, systems, devices, software, or services that include embedded or incidental information technology).
[49] See 41 USC 1326 (a) (1)
[50] 41 USC 4713

appendix. The FASCSA requires the Federal Acquisition Regulatory (FAR) Council to prescribe such regulations as may be necessary to carry out this section. NIST does and will continue to work closely with interagency colleagues within the FASC and the federal acquisition community to help ensure harmonized guidance.

This appendix does not provide guidance on how to conduct an assessment, which is best addressed through role-based training, education, and work experience. NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*, is also a recommended reference. Agencies should take steps to ensure that personnel with current and prospective responsibilities for performing SCRAs have adequate skills, knowledge, and depth and breadth of experience sufficient to identify and discern indications of cybersecurity risk in the supply chain and the assessment of those risks. Agencies are strongly encouraged to invest in training to grow and sustain competencies in analytic skills and SCRM knowledge. Counter-intelligence and security training are also strongly recommended for C-SCRM PMO staff or those personnel with responsibilities dedicated to performing SCRAs. Building this capability helps to ensure that there is sufficient understanding and awareness of adversarial-related supply chain risks in the workforce while also developing a risk management cadre to provide advice and support for risk response decisions and actions.

Relationship to NIST SP 800-161, Rev. 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*

The practices and processes to assess, respond to, and otherwise manage cybersecurity risks in the supply chain are discussed at length throughout the main body and appendices of NIST SP 800-161, Rev. 1. This appendix provides supplemental expanded guidance that is tailored and applicable to federal agencies. This guidance describes the scope and type of supply chain risk assessment information and documentation used to support and advise risk response decisions and actions, both internally to senior agency officials and externally to bodies such as the FASC.

This augmented guidance is also intended to ensure a baseline consistency and sufficiency of processes and SCRI utilized for assessment and documentation and to facilitate information sharing and recommendations to applicable decision makers, whether at a given agency or at the government-wide level. Within the constraints of requisite support for federal enterprise-level analysis and decision-making, agencies continue to have the flexibility to assess and manage their supply risk in a manner consistent with the broader guidance outlined in the main body and other appendices of NIST SP 800-161, Rev.1 and their policies, mission and priority needs, and existing practices (to the extent that these are sufficient).

FASCSA Supply Chain Risk Definition vs. NIST SP 800-161, Rev. 1, *Cybersecurity-Supply Chain Risk Definition*

Agencies should take note that the FASCSA definition of supply chain risk is narrowly focused on risk that arises from an assessment that there is intent and capability by an adversarial threat actor to conduct malicious activity or otherwise cause malicious harm. In contrast, NIST's definition and scope of cybersecurity supply chain risk is otherwise consistent with the FASCSA definition but broader in scope as it includes both adversarial and non-adversarial-related risks. Consistent with the FASCSA's direction that agencies rely upon NIST standards and guidance, agencies need to ensure that their assessment and risk response activities address all applicable cybersecurity risks throughout the supply chain.

SUPPLY CHAIN RISK ASSESSMENTS (SCRAs)

General Information

The FASCSA requires agencies to conduct and prioritize supply chain risk assessments when acquiring a covered article as well during its use or performance. In most cases, this also compels the need to assess the source associated with the covered article. Supply chain risk assessments conducted by agencies are highly dependent on the operating environment and use case associated with a covered article. Agencies have flexibility in how they apply NIST guidelines to their operations and there is not – nor should there be – a one-size-fits-all approach to conducting a SCRA. However, to facilitate assessments that may need to take place at the government-wide level to evaluate risks that may impact national security or multiple agency missions, there is a need to ensure that agencies' SCRA information and documentation reflect an acceptable baseline level of due diligence and standardization.

In general, information used for an assessment will be comprised of up to three categories of inputs:

1) Purpose and context information (i.e., use-case specific) used to understand the risk environment and to inform and establish risk tolerance relative to the use case
2) Data or information obtained from the source
3) All-source information, which may come from publicly available data, government sources (may include classified sources), and/or commercial fee-based sources

The purpose and context, as well as when an assessment of a supplier and/or covered article is performed in the SDLC or procurement life cycle, will drive variations in terms of focus and scope with regard to what type, how much, and from what sources information used in an assessment is obtained.

The FASCSA recognizes that agencies have constrained resources, but it is necessary to prioritize the conduct of SCRAs.[51] Prioritization is not meant to be understood as only a subset of sources or covered articles that should be assessed. Rather, agencies should establish a tiered

[51] See Section 1326 (a)(2) of the FASCSA.

set of priority levels commensurate with the criticality and potential for risk impact. This tiering can then be used to guide or compel the timing of, order, scope, and frequency of SCRAs.

In addition to externally driven priorities (e.g., government-wide policy direction, regulatory requirement, etc.) and agency-defined prioritization factors, NIST SP 800-161, Rev 1. instructs agencies to prioritize assessments concerning critical suppliers (i.e., sources) and critical systems and services, as compromise of these sources and covered articles is likely to result in greater harm than something determined to be non-critical. For these assessments, agencies should address all baseline risk factors described in the Baseline Risk Factors (common, minimal) section below (augmenting and weighing the factors, as appropriate to the use case, to ensure appropriate consideration of both adversarial and non-adversarial-related risks). For a given non-critical source or non-critical covered article, agencies have discretion – consistent with their own internal policies and practices and absent other mandates – as to whether all, some, and to what extent the baseline risk factors described in this appendix should be considered when assessing supply chain risk. However, if and when there are one or more credible findings that indicate that a substantial supply chain risk may or does exist (see Supply Chain Risk Severity Schema, described below), it may require that a more comprehensive assessment be completed, inclusive of all of the baseline risk factors or more robust research and analysis of the baseline risk factors. (See the risk response guidance described in the Risk Response Section below.)

The responsibility and accountability for determining the priority levels for SCRAs, evaluating impact, making risk response decisions, and taking actions based on the findings in a SCRA are inherently governmental functions and cannot be outsourced. However, some agencies may rely on a qualified third party for support in conducting research, documenting findings, and reviewing relevant information. To aid in their research and assessment activities, agencies may also acquire access to commercially available data or tools. Appropriate requirements should be included in solicitations and contracts to address access to, handling, and safeguarding SCRI. Failure to do this, in and of itself, reflects a security control gap and creates an unmitigated supply chain risk. Moreover, such a gap can undermine the entire purpose of an agency's SCRA efforts or even facilitate the success of foreign adversaries' malicious actions against the United States. Additionally, agency personnel should follow the guidance and direction of their ethics officials and legal counsel to ensure that protections are in place to guard against conflicts of interest and inappropriate or unauthorized access to or disclosure of information, as SCRI may be sensitive, proprietary, or – in certain instances – classified. For the latter category of information, agencies must ensure adherence to laws, policies, and procedures governing classified information and limit access to only those personnel who have the proper clearance, authorized access, and need to know.

In all instances, personnel who support the conduct of an assessment have a duty and responsibility to act prudently and objectively and to exercise reasonable care in researching and analyzing a source or covered article as this SCRI underpins subsequent risk response decisions and actions.

Baseline Risk Factors (Common, Minimal)

This section describes the baseline (common, non-exclusive) supply chain risk factors and guidance that agencies should incorporate into (or map to the factors included in) their agency-

defined SCRA methodology. These factors are to be used as a guide to research, identify, and assess risk for those SCRAs pertaining to critical sources or critical covered articles, at a minimum. A common baseline of risk factors also helps to ensure that due diligence is consistently conducted as part of the analysis that informs risk response decisions and actions, whether these occur at various levels within an agency or at the federal enterprise-level. Agencies should assess additional factors beyond the baseline factors, as deemed relevant and appropriate to a given assessment use case.

Objectives for establishing this baseline set of factors include:

- Level setting evaluations for sources and covered articles;
- Ensuring that the minimum necessary information is available to the FASC, when required;
- Promoting consistency and comparability across agencies;
- Aiding the conduct of more sophisticated analyses, such as trend analysis or causal or correlation relationships between identified indicators of risk and realized risks; and
- Establishing and maintaining a base of information sufficient to identify and understand potential mitigation options and inform prioritization or risk response trade-off analysis/decisions.

Table E-1 that follows includes a list of the baseline risk factors and their corresponding definition or description. These factors are also consistent with and align to the factors included in the FASC Final Rule.[52] The right-most column includes a list of the type of information that may be identified and found to be an indicator of risk. This list is intended to be used as a reference aid and is not all-inclusive of the possible indicators of risk. Information that pertains to context-based risk factors should be known by the agency and is often already documented (e.g., in a system security plan or acquisition plan). An assessment of these use case-specific and context-based factors helps to understand inherent risk,[53] guides the identification and selection of needed cybersecurity and SCRM controls and procurement requirements, and aids in determining the risk tolerance threshold for a covered article associated with a given use case.

The next set of vulnerability and threat risk factors is focused on risk that may be inherited from the covered article itself or the associated source or supply chain. Agencies will assess the findings associated with these baseline (and any additional) factors to provide an informed judgment about whether there are indications of threat from an adversarial threat actor, the likelihood for compromise or harm and resultant impact, and whether the assessed risk pertaining to a source and/or covered article is within or exceeds their acceptable risk tolerance level.

[52] CFR Part 201-1.300 Evaluation of Sources and Covered Articles
[53] Inherent risk, defined for this purpose, is the current risk level given the existing set of controls.

Table E-1: Baseline Risk Factors

Baseline Risk Factor	Definition or Guidance	Non-exclusive Indicators of Risk (as applicable)
Use-Case/Context (Inherent Risk)		
Purpose	Understand the requirement for product or service and how it will be or is being used.	• Options available in the marketplace to fulfill need • Urgency of need • Duration of need
Criticality	Identify if the product, service, or source is deemed a critical system, system component, service, or supplier. Refer to the main body and glossary of NIST SP 800-161, Rev. 1 for additional guidance. Also see Appendix F for information regarding EO-critical software.	• Supplier or covered article (or component therein) performs or is essential to (or, if compromised, could result in harm to) a mission-critical function, life safety, homeland security, critical infrastructure, or national security interest or has an interdependency with another covered article performing or essential to such functions
Information and Data	Understand and document the type, amount, purpose, and flow of federal data/information used by or accessible by the product, service, and/or source.	• Requirement or ability to access CUI or classified information • Federal information will be managed and/or accessible for external persons or entities other than the prime contractor or supplier • Product or service data inputs or outputs can affect life safety if compromised
Reliance on the covered article or source	Understand and articulate the degree to which an agency is reliant on a covered article and/or source and why.	• Prevalence of use of the product or service by the agency • Single source of supply • Product or service availability in the marketplace • Availability of (or acceptable alternatives to) the product, service, or source

Baseline Risk Factor	Definition or Guidance	Non-exclusive Indicators of Risk (as applicable)
User/operational environment in which the covered article is used or installed or service performed	For products included in systems or as a system component, the user environment should be described in the System Security Plan and/or C-SCRM System Plan. For labor-based services, understand and document relevant information about the user environment (i.e., place of performance) that may expose the agency to risk.	• The system and/or C-SCRM Security Plan should identify and document risks and describe the applicable, selected security controls implemented or required to be implemented to mitigate those risks • Relevant environment considerations that give rise to risk concerns should be documented in procurement plans and applicable controls addressed in solicitations and contracts
External agency interdependencies	Understand and identify interdependencies related to data, systems, and mission functions.	• Covered article performs a function in support of a government-wide shared service • Covered article exchanges data with another agency's mission critical system • Contractor maintains an analytic tool that stores government-wide CUI data
Vulnerabilities or Threats (Inherited Risk)		
Functionality, features, and components of the covered article	Information informs a determination as to whether the product or service is fit for purpose" and the extent to which there is assurance that the applicable C-SCRM dimensions (see Section 1.4 of main body) are satisfied, and/or there are inherent or unmitigated weaknesses or vulnerabilities.	• Ability of the source to produce and deliver the product or service as expected • Built-in security features and capabilities or lack thereof • Who manages or has ultimate control over security features • Secure configuration options and constraints • Management and control of security features (who, how) • Network/internet connectivity capability or requirements and methods of connection • Software and/or hardware bill of material

Baseline Risk Factor	Definition or Guidance	Non-exclusive Indicators of Risk (as applicable)
		• Any transmission of information or data (to include, if known) the identification of the source and location of the initiator or recipient of the transmission) to or by a covered article necessary for its function
Company (i.e., source) Information	Information about the company, to include size, structure, key leadership, and its financial health.	• Corporate family tree • Years in business • Merger and acquisition activity (past and present) • Contracts with foreign governments • Customer base and trends • Association or previous experience by company leadership (Board or C-suite in foreign government or military service) • Stability or high turnover or firings at senior leadership level • Number of employees at specific location and company-wide • Investors/investments • Patent sales to foreign entities • Financial metrics and trends • Financial reports/audits
Quality/Past Performance	Information about the ability of the source to produce and deliver covered articles as expected. This includes an understanding of the quality assurance practices associated with preventing mistakes or defects in manufactured/ developed products and avoiding problems when delivering solutions or services to customers.	• Past performance information • Relevant customer ratings or complaints • Recalls • Quality metrics • Evidence of a quality program and/or certification

Baseline Risk Factor	Definition or Guidance	Non-exclusive Indicators of Risk (as applicable)
Personnel	Information about personnel affiliated with or employed by the source or an entity within the supply chain of the product or service.	• The supplier's program to vet its personnel, to include whether there is an insider threat program, and/or whether the supplier performs background checks and prior employment verification • Hiring history from a foreign country or foreign adversary's intelligence, military, law enforcement or other security services • Turnover rate • Staffing level and competencies • Evidence of questionable loyalties and unethical or illicit behavior and activities
Physical	Information associated with the physical aspects of the environment, structures, facilities, or other assets sufficient to understand if/how they are secured and the consequences if damaged, unavailable, or compromised.	• Evidence of the effectiveness of physical security controls, such as procedures and practices that ensure or assist in the support of physical security • Proximity to critical infrastructure or sensitive government assets or mission functions • Natural disasters or seismic and climate concerns
Geopolitical	Information associated with a geographic location or region of relevance to the source or the supply chain associated with the source, product, and/or service.	• Location-based political upheaval or corruption • Trade route disruptions • Jurisdictional legal requirements • Country or regional instability
Foreign Ownership, Control, or Influence (FOCI)	Ownership of, control of, or influence over the source or covered article(s) by a foreign interest (e.g., foreign government or parties owned or controlled by a foreign government, or other ties between the source and a foreign	• Country is identified as a foreign adversary or country of special concern • Source or its component suppliers have headquarters, research, development, manufacturing, testing, packaging, distribution, or service facilities or other operations in a foreign country, including a country of special concern or a foreign adversary

Baseline Risk Factor	Definition or Guidance	Non-exclusive Indicators of Risk (as applicable)
	government) has the power, direct or indirect, whether or not exercised, to direct or decide matters that affect the management or operations of the company.	• Identified personal and/or professional ties between the source – including its officers, directors or similar officials, employees, consultants, or contractors – and any foreign government • Implications of laws and regulations of any foreign country in which the source has headquarters, research development, manufacturing, testing, packaging, distribution, or service facilities or other operations • Nature or degree of FOCI on a supplier • FOCI of any business entities involved in the supply chain, to include subsidiaries and subcontractors, and whether that ownership or influence is from a foreign adversary of the United States or country of concern • Any indications that the supplier may be partly or wholly acquired by a foreign entity or a foreign adversary • Supplier domiciled in a country (without an independent judicial review) where the law mandates cooperation, to include the sharing of PII and other sensitive information, with the country's security services • Indications that demonstrate a foreign interest's capability to control or influence the supplier's operations or management or that of an entity within the supply chain • Key management personnel in the supply chain with foreign influence from or with a connection to a foreign government official or entities, such as members of the board of directors, officers, general partners, and senior management official • Foreign nationals or key management personnel from a foreign country involved with the design, development,

Baseline Risk Factor	Definition or Guidance	Non-exclusive Indicators of Risk (as applicable)
		manufacture or distribution of the covered article • Supplier's known connections to a foreign country or foreign adversary's intelligence, law enforcement, or other security service • Supplier is domiciled in or influenced/controlled by a country that is known to conduct intellectual property theft against the United States
Compliance/Legal	Information about non-compliance, litigation, criminal acts, or other relevant legal requirements	• Record of compliance with pertinent U.S. laws, regulations, contracts, or agreements • Sanctions compliance • Trade controls compliance • Judgments/Fines
Fraud, Corruption, Sanctions, and Alignment with Government Interests	Information about past or present fraudulent activity or corruption and being subject to suspension, debarment, exclusion, or sanctions (also see Table E-2 and discussion immediately preceding table)	• Civil or criminal litigation • Past history or current evidence of fraudulent activity • Source's history of committing intellectual property theft • Supplier's dealings in the sale of military goods, equipment, or technology to countries that support terrorism or proliferate missile technology or chemical or biological weapons and transactions identified by the Secretary of Defense as "posing a regional military threat" to the interests of the United States • Source's history regarding unauthorized technology transfers
Cybersecurity	Information about the cybersecurity practices, vulnerabilities, or incidents of the source, product, service, and/or supply chain	• Evidence of effective cybersecurity policies and practices • Supplier's history as a victim of computer network intrusions • Supplier's history as a victim of intellectual property theft • Information about whether a foreign intelligence entity unlawfully collected or attempted to acquire an acquisition

Baseline Risk Factor	Definition or Guidance	Non-exclusive Indicators of Risk (as applicable)
		item, technology, or intellectual property • Existence of unmitigated cybersecurity vulnerabilities • Indication of malicious activity – including subversion, exploitation, or sabotage – associated with the supplier or the covered article • Any unauthorized transmission of information or data by a covered article to a country outside of the United States
*Counterfeit and Non-Conforming Products (include in baseline if relevant to source and/or product being assessed; if in doubt, include)	Information about counterfeits, suspected counterfeits, gray market, or non-conforming products	• Evidence or history of counterfeits or non-conforming products associated with the supplier • Suppliers' anti-counterfeit practices and controls • Sourcing of components from the gray market
Supply Chain Relationships, Visibility, and Controls	Information about the supply chain associated with the source and/or covered article.	• Evidence of effective C-SCRM and supplier relationship management practices • Components or materials (relevant to covered article) originate from single source in upstream supply chain • Reliance on single trade route • Provenance of the product

Information about these baseline risk factors should be generally available from open sources, although the type, quality, and extent of information is likely to vary broadly. In some instances, no information may be discovered or deemed to be applicable for a given factor and should be noted accordingly. Research should be tailored toward attaining credible information of greatest relevance to the purpose and context for which the assessment is being conducted (see discussion about information quality in the Assessment Documentation and Records Management section below). Because of these variables, it is not possible nor desirable to attempt to standardize below the risk factor level.

Findings associated with these factors may reflect a mix of information about objective facts, threats, vulnerabilities, or general "exposures" that, when assessed discretely or in aggregate, indicate risk being possible or present. The findings may also be positive, neutral, or negative in nature. Positive findings are indicative of the source or covered article having desired or required assurance attributes. Negative findings indicate that there is or may be a risk that presents

concern and for which a determination needs to be made as to whether the risk is within tolerance, requires mitigation, and/or may compel the need for information sharing with the FASC.

Caution! The existence of one or more risk indicators associated with the above factors does not necessarily indicate whether a source, product, or service poses a viable or unacceptable risk, nor does it indicate the severity of the risk. Care should also be taken to analyze what combination of factors and findings may give rise to risk or, conversely, mitigate risk concerns. Uncertainty about a risk determination may prompt the need to conduct additional due diligence research and analysis, escalate internally or externally, or seek advice as to whether the risk is such that mitigation is not possible.

Separate from or as part of the assessment, agencies should examine whether there are any laws or federal restrictions that prohibit the use of certain suppliers and the acquisition or use of certain items, services, or materials. The list below, while not inclusive of all applicable laws and restrictions, is focused on foreign ownership and control, other types of foreign influence, foreign adversaries, and foreign investment concerns that may pose risks to the U.S. supply chain.

The use of such suppliers or the acquisition of such an item, service, or material from an individual or entity in any of the lists below is a violation of law absent an exception or waiver and should, therefore, be excluded from the federal procurement process. If an item has already been obtained prior to the below prohibitions going into effect, agencies should conduct an assessment to determine whether they are permitted to keep the prohibited items or services and, if so, whether any adversarial threats posed by continued use can be mitigated.

1. **The Specially Designated Nationals (SDN) and Blocked Persons List:** The Treasury Department, Office of Assets Control (OFAC), through EO 13694 and as amended by EO 13757, provided for the designation on the Specially Designated Nationals and Blocked Persons List (SDN List) of parties determined to be responsible for, complicit in, or to have engaged in, directly or indirectly, malicious cyber-enabled activities. Any entity in which one or more blocked persons directly or indirectly holds a 50 % or greater ownership interest in the aggregate is itself considered blocked by operation of law. U.S. persons may not engage in any dealings, directly or indirectly, with blocked persons.
2. **The Sectoral Sanctions Identifications (SSI) List:** The sectoral sanctions imposed on specified persons operating in sectors of the Russian economy identified by the Secretary of the Treasury were done under EO 13662 through Directives issued by OFAC pursuant to its delegated authorities. The SSI List identifies individuals who operate in the sectors of the Russian economy with whom U.S. persons are prohibited from transacting with, providing financing for, or dealing in debt with a maturity of longer 90 days.
3. **The Foreign Sanctions Evaders (FSE) List:** OFAC publishes a list of foreign individuals and entities determined to have violated, attempted to violate, conspired to violate, or caused a violation of U.S. sanctions on Syria or Iran pursuant to EO 13608. It also lists foreign persons who have facilitated deceptive transactions for or on behalf of persons subject to U.S. sanctions. Collectively, such individuals and companies are called “Foreign

Sanctions Evaders" or "FSEs." Transactions by U.S. persons or within the United States involving FSEs are prohibited.
4. **The System for Award Management (SAM) Exclusions:** The SAM contains the electronic roster of debarred companies excluded from federal procurement and non-procurement programs throughout the U.S. Government (unless otherwise noted) and from receiving federal contracts or certain subcontracts and from certain types of federal financial and non-financial assistance and benefits. The SAM system combines data from the Central Contractor Registration, Federal Register, Online Representations and Certification Applications, and the Excluded Parties List System. It also reflects data from the Office of the Inspector General's exclusion list (GSA) (CFR Title 2, Part 180).
5. **The List of Foreign Financial Institutions Subject to Correspondent Account Payable-Through Account Sanctions (the "CAPTA List"):** The CAPTA List replaced the list of Foreign Financial Institutions Subject to Part 561. It includes the names of foreign financial institutions subject to sanctions, certain prohibitions, or strict conditions before a U.S. company may do business with them.
6. **The Persons Identified as Blocked:** Pursuant to 31 CFR 560 and 31 CFR 560.304, property and persons included on this list must be blocked if they are in or come within the possession or control of a U.S. person.
7. **The BIS Unverified List:** Parties listed on the Unverified List (UVL) are ineligible to receive items subject to the Export Administration Regulations (EAR) by means of a license exception.
8. **The 2019 National Defense Authorization Act, Section 889:** Unless a waiver is granted, NDAA Section 889 prohibits the Federal Government, government contractors, and grant and loan recipients from procuring or *using* certain "covered telecommunication equipment or services" that are produced by Huawei, ZTE, Hytera, Hikvision, Dahua, and their subsidiaries as a "substantial or essential component of any system or as critical technology as part of any system."
9. Any other federal restriction or law that would restrict the acquisition of goods, services, or materials from a supplier.

Risk Severity Schema

A common framework is needed as a reference to aid agencies in determining an appropriate risk response to the results of an SCRA. This schema indicates whether an identified risk associated with a given source or covered article can be managed within agency-established C-SCRM processes or requires internal or external escalation for a risk-response decision or action.

There is benefit in adopting and tailoring an existing government-wide severity schema as this creates a degree of alignment and consistency with other related processes and guidance that are already in use. The Supply Chain Risk Severity Schema (SCRSS) introduced and described below mirrors the intent and structure of the Cyber Incident Severity Schema (CISS), which was developed in coordination with departments and agencies with a cybersecurity or cyber operations mission.

Similar to the CISS but focused on and tailored to supply chain risks versus cyber incidents, the SCRSS is intended to ensure a common view of:

- The severity of assessed supply chain risk associated with a given source or covered article,
- The urgency required for risk response,
- The seniority level necessary for coordinating or making a risk response decision, and
- The information, documentation, and processes required to inform and support risk response efforts.

Table E-2: Risk Severity Schema

Level	Type	Description
5	Urgent National Security Interest Risk	Adversarial-related risk with imminent or present impact to national security interests
4	National Security Interest Risk	Adversarial-related risk with potential to impact national security interests
3	Significant Risk	Adversarial-related risk with potential to impact multiple agencies
2	Agency High Risk	Non-adversarial-related "high" risk associated with an agency's critical supplier (i.e., source), system, component, or high value asset
1	Agency Low or Moderate Risk	Assessed risk that does not meet the description for any of the other four risk levels

The schema in Table E-2 is not intended to replace existing agency-established methodologies that describe and assign various risk levels or scores. Rather, it is to be used as a mapping reference that associates an agency risk assessment result to the schema level that most closely describes that result. Mapping gives agencies the flexibility they need to assess and describe risk levels in a manner applicable to their purpose and context while also creating a normalized lexicon to commonly describe supply risk severity across the federal enterprise. This schema framework also helps to communicate expectations about risk response coordination, information sharing, and decision-making responsibilities associated with each level.

Risk Response Guidance

Depending on the SCRSS level of an assessed supply chain risk, agencies may need to escalate and share SCRA information with others within their internal organization for further research, analysis, or risk response decisions or engage with external officials, such as the FASC.

Information Sharing

Supply chain risks assessed at Levels 3 and above are characterized as "substantial risk," per the FASC rule, and require mandatory information sharing with the FASC via the Information

Sharing Agency[54] (ISA) for subsequent review and potential additional analysis and action. At their discretion, agencies may choose to voluntarily share information concerning identified Level 2 or Level 1 risks with the FASC supply chain, in accordance with FASC information-sharing processes and requirements.

SCRI that is identified or received outside of an assessment process may also compel the need for mandatory or voluntary sharing with the FASC or another government organization, such as the FBI, FCC, or DHS CISA. Examples of such information include but are not limited to information about a supply chain event, supply chain incident, information obtained from an investigatory organization (e.g., the Office of Inspector General), or an anonymous tip received through an agency hotline.

All information sharing that occurs between an agency and the FASC, whether mandatory or voluntary, is to be done in accordance with FASC-established information sharing requirements and processes consistent with the authorizing statute and regulations. Additionally, agencies should designate a senior agency official to be the liaison for sharing information with the FASC. Agencies should establish processes for sharing (sending and receiving) information between the agency and the FASC and establish commensurate requirements and processes tailored to their organization for sharing SCRI within their own organization.

Note: The FASC may issue updated or additional guidance concerning the circumstances and criteria for mandatory and voluntary information sharing. Agencies should refer to and follow the most current FASC guidance.

Risk Response Escalation and Triaging

Agencies are reminded of the importance of integrating SCRM into enterprise risk management activities and governance, as covered extensively in the main body and appendices of NIST SP 800-161, Rev. 1. For risk that is determined to be at a SCRSS substantial level, it is necessary to escalate the risk assessment information to applicable senior level officials within the agency, including legal counsel. Agencies should also ensure that appropriate officials have sufficient security clearances to allow them to access classified information, as needed and appropriate, to inform or support risk response coordination, decisions, or actions.

Because a risk deemed to be substantial is adversarial in nature, there may also be law enforcement, counter-intelligence equities, legal implications, or existing activities that need to be considered prior to responding to the assessed risk or engaging or communicating with the source. Agencies' sharing of substantial risk information with the FASC standardizes and streamlines the process that agencies should follow to ensure these risks are "triaged" appropriately.

[54] The Department of Homeland Security (DHS), acting primarily through the Cybersecurity and Infrastructure Security Agency, has been designated to serve as the FASC's ISA. The ISA performs administrative information sharing functions on behalf of the FASC, as provided at 41 U.S.C. 1323 (a) (3).kk

ASSESSMENT DOCUMENTATION AND RECORDS MANAGEMENT

Content Documentation Guidance

Agencies need to ensure that their assessment record satisfies the minimal documentation requirements described in this section for the mandatory sharing of information about sources and/or covered articles to the FASC or when escalating internally for risk-response decisions that may implicate the use of an agencies' Section 4713 authority. This documentation baseline standard helps to ensure that a robust and defensible record is or can be established to support well-informed risk response decisions and actions. It also helps to promote consistency in the scope and organization of documented content to facilitate comparability, re-usability, and information sharing.

The documentation requirements extend beyond capturing risk factor assessment information and include general facts about who conducted the assessment and when, identifier and descriptive information about the source and covered article, citation of the data sources used to attain assessment information, an assignment of a confidence level to discrete findings and aggregate analysis of findings, and noting assumptions and constraints.

Agencies should also have and follow a defined assessment and risk determination methodology. This methodology should be documented or referenced in the assessment record concerning a given source and/or covered article. Any deviations from the agency-defined methodology should be described in the general information section of the assessment record.

As information is researched and compiled, it needs to be organized and synthesized to cull out and document relevant findings that align with the varying risk factor categories. Sourced information (including contextual metadata), especially notable findings of risk of concern, should retain or be retrievable in a form that retains its informational integrity and considered as supplemental content that may be required to support and defend a risk response decision or action. As such, the sources for, the quality of, and the confidence in the sourced information need to be considered as part of the assessment activity and documented accordingly. Broadly, quality information should be timely, relevant, unbiased, sufficiently complete or provided in-context, and attained from credible sources.

Documentation requirements should be incorporated into existing, relevant supply chain risk assessment policies, processes, and procedures. These requirements should be informed by consultation with and direction from officials within the agency, to include legal counsel and personnel with responsibilities for records management, CUI and classified information management, and privacy.

While a format is not specified, the minimal scope of content and documentation for a given assessment record should include the content described in Table E-3 below:

Table E-3: Assessment Record – Minimal Scope of Content and Documentation

General Information	Additional Comments
Agency responsible for the assessment	Agencies should be able to identify points of contact and retain information about any non-federal personnel who supported the assessment, tools, and/or data sources (inclusive of commercially obtained) used in support of the assessment.
Date of assessment or time frame in which the assessment was conducted	Agencies should note which of their findings are temporal in nature and subject to change over time.
Source Profile: Identifier and Descriptive Information about Assessed Supplier	Document (as knowable and applicable) the supplier's legal name, DBA name, domicile, physical address, and (if different) the physical location of HQ; DUNS number and CAGE Code; contact phone number; registered as foreign or domestic company; company website URL, company family tree structure, and location in company family tree (if known); company size; years in business; and market segment.
Identifier and descriptive information about assessed covered article	Document the product name, unique identifier (e.g., model number, version number, serial number), relevant NAICS and PSC, and a brief description.
Summary of purpose and context of assessment	Identify the applicable life cycle phase indicated when the assessment occurred (e.g., market research, procurement action, operational use).
Assessment methodology	Reference the documented methodology, and describe any deviations from it.
Source or covered article research, findings, and risk assessment results	Document the analysis of findings, identification, and assessment of risk. Minimally, there should be a summation of the key findings, an analysis of those findings, and a rationale for risk level determination. This summary should address potential or existing threats (whether and why they are assessed as adversarial, non-adversarial, or indeterminate in nature) or vulnerabilities of the source, covered article, and the associated supply chain. Include notes about relevant assumptions and constraints.
Impact assessment	Relative to the purpose and context of the assessment, describe the assessed potential for impact given the type, scope, and severity of the identified risk.

General Information	Additional Comments
Mitigation of unresolved or unacceptable risks	Include a discussion of the capability, capacity, and willingness of the source to mitigate risks to a satisfactory level and/or the capability and capacity of the agency to mitigate risks. Identify viable mitigation options, if known, to address any unresolved or unacceptable risks.
Assessment of risk severity level in accordance with supply chain risk severity schema	Include the SCRSS level number and an explanation for why this level was assigned. Address identified implications for government missions or assets, national security, homeland security, or critical functions associated with use of the source or covered article.
Risk response	Describe risk response decisions or actions taken (e.g., avoid, mitigate, escalate to FASC for coordination and triaging).
Any other information, as specified and directed to provide by the FASC or is included per agency discretion	Describe or provide information that would factor into an assessment of supply chain risk, including any impact to agency functions and other information as the FASC deems appropriate.
Review and clearance	Ensure that the credibility of and confidence in the sources and available information used for risk assessment associated with proceeding, using alternatives, and/or enacting mitigation efforts is addressed. Confirm that the assessment record was reviewed and cleared by applicable officials, to include applicable Senior Leadership and legal counsel, for risk assessed as being substantial. Review and clearance are also intended to ensure that the assessment record and supporting information are appropriately safeguarded, marked, and access-controlled.

Assessment Record

Agencies should ensure that records management requirements are adhered to with regard to SCRAs and supporting artifacts. Policies and procedures should be in place that address the requisite safeguarding, marking, handling, retention, and dissemination requirements and restrictions associated with an assessment record and its associated content.

If and when assessment services (e.g., analytic support) or commercially-provided information are obtained to support the development of an assessment record, an agreement (e.g., contract, interagency agreement) should specify appropriate requirements and restrictions about scope, the purpose of data use, and limitations, access, disposal, and retention rights.

APPENDIX F: RESPONSE TO EXECUTIVE ORDER 14028's CALL TO PUBLISH GUIDELINES FOR ENHANCING SOFTWARE SUPPLY CHAIN SECURITY

Departments and agencies seeking to implement Cybersecurity Supply Chain Risk Management in accordance with Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, should reference NIST's dedicated EO 14028 web-based portal at https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity. This guidance has been moved online in order to:

- Co-locate it with related EO guidance under NIST's purview;
- Enable updates to reflect evolving guidance without directly impacting SP 800-161, Rev. 1; and
- Provide traceability and linkage with other NIST web-based assets as they move online to encourage dynamic and interactive engagement with stakeholders.

APPENDIX G: C-SCRM ACTIVITIES IN THE RISK MANAGEMENT PROCESS[55]

Risk management is a comprehensive process that requires enterprises to: 1) frame risk (i.e., establish the context for risk-based decisions), 2) assess risk, 3) respond to risk once determined, and 4) monitor risk on an ongoing basis using effective enterprise communications and a feedback loop for continuous improvement in the risk-related activities of enterprises. Figure G-1 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 enterprise, mission, and operations levels.

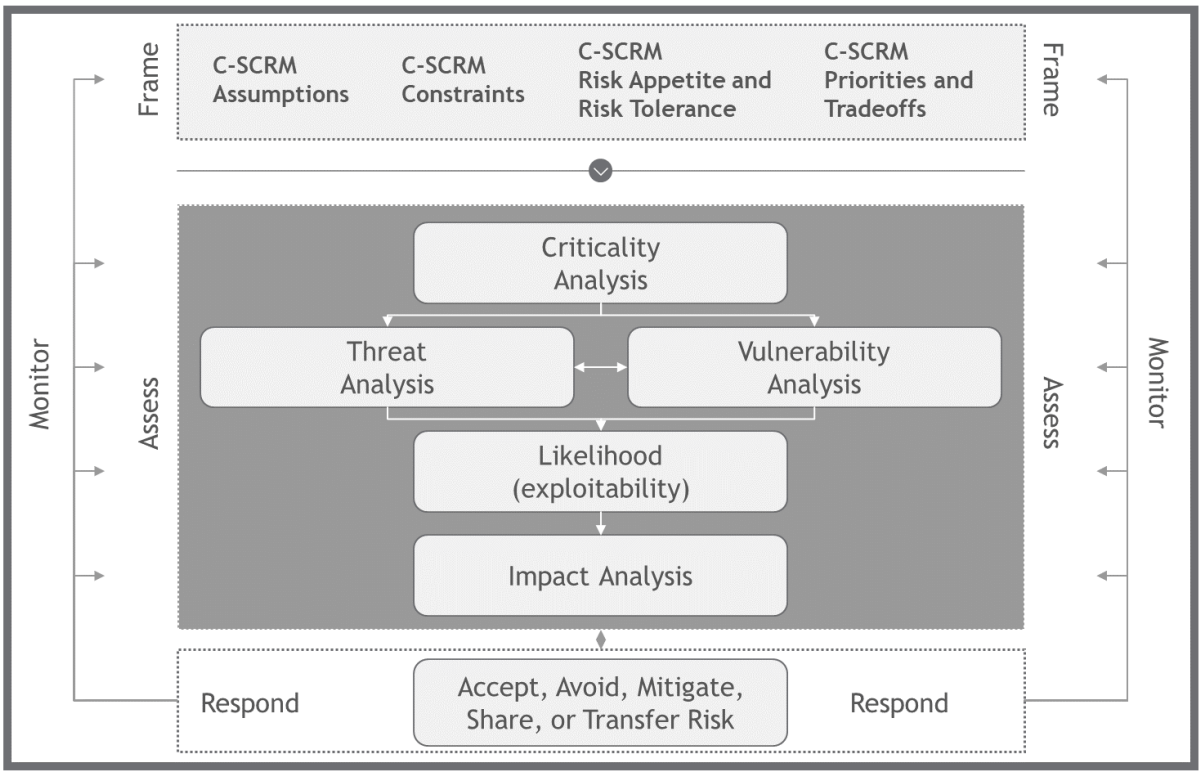

Fig. G-1: Cybersecurity Supply Chain Risk Management (C-SCRM)

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. Enterprises 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 G-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 the simultaneous flow of information and guidance among the steps.

[55] Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, *Improving the Nation's Cybersecurity*.

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.

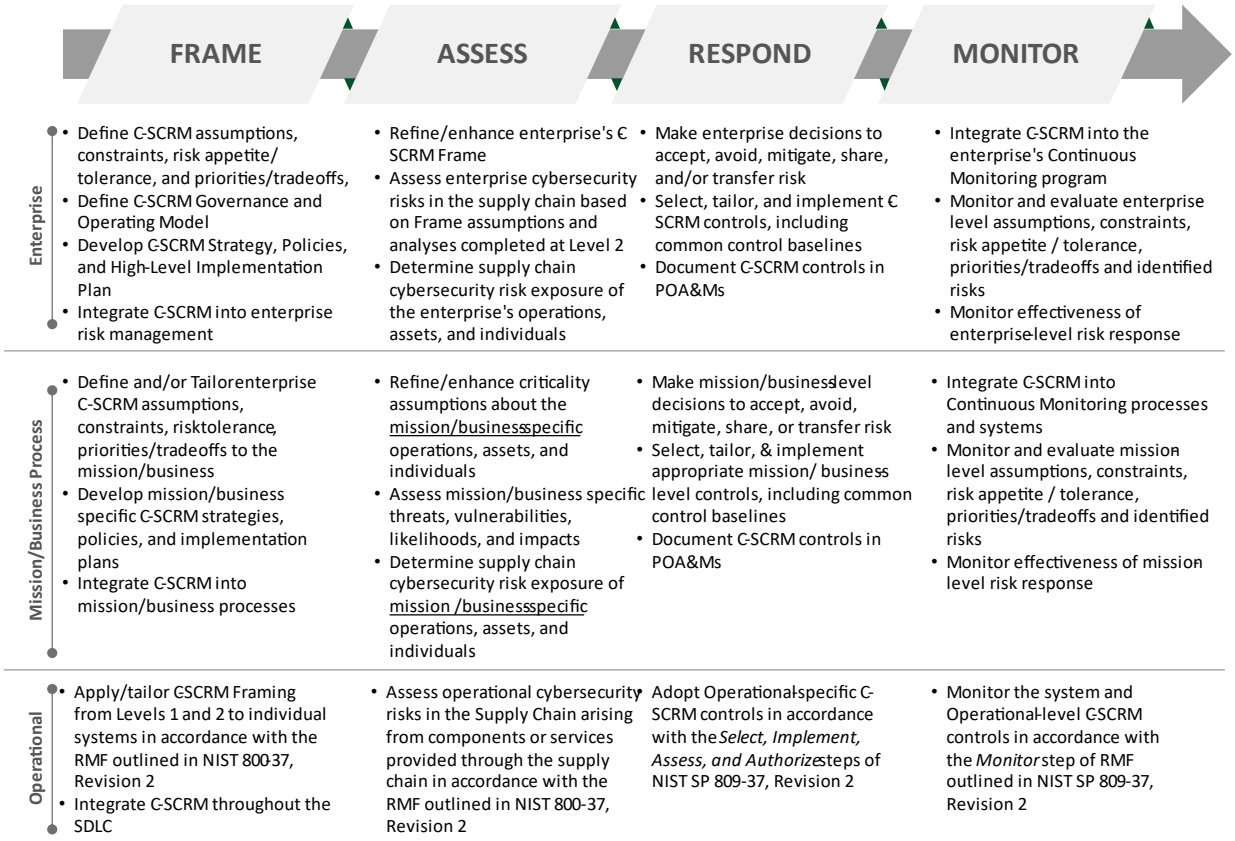

Fig. G-2: C-SCRM Activities in the Risk Management Process

Figure G-2 depicts interrelationships among the risk management process steps, including the order in which each analysis is executed and the interactions required to ensure that the analysis is inclusive of the various inputs at the enterprise, mission and business process, and operational levels.

The remainder of this section provides a detailed description of C-SCRM activities within the Frame, Assess, Respond, and Monitor steps of the Risk Management Process. The structure of subsections Frame through Monitor mirrors the structure of [NIST SP 800-39], Sections 3.1-3.4. For each step of the Risk Management Process (i.e., Frame, Assess, Respond, Monitor), the structure includes Inputs and Preconditions, Activities, and Outputs and Post-Conditions. Activities are further organized into Tasks according to [NIST SP 800-39]. [NIST SP 800-161, Rev 1.] cites the steps and tasks of the risk management process, but rather than repeating any other content of [NIST SP 800-39], it provides C-SCRM-specific guidance for each step with its Inputs and Preconditions, Activities with corresponding Tasks, and Outputs and Post-Conditions. This document adds one task to those provided in [NIST SP 800-39] under the Assess step: Task 2-0, *Criticality Analysis*.

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 enterprise (e.g., C-SCRM PMO Processes, Enterprise Risk Management, Mission and Business Process Risk Managers, etc.). Other personnel or entities are free to make use of the guidance as appropriate to their situation.

ENTERPRISE-WIDE RISK MANAGEMENT AND THE RMF

Managing cybersecurity risks throughout the supply chain requires a concerted and purposeful effort by enterprises across enterprise, mission and business process, and operational levels. This document describes two different but complementary risk management approaches that are iteratively combined to facilitate effective risk management across the three levels.

The first approach is known as FARM and consists of four steps: Frame, Assess, Respond, and Monitor. FARM is primarily used at Level 1 and Level 2 to establish the enterprise's risk context and inherent exposure to risk. Then, the risk context from Level 1 and Level 2 iteratively informs the activities performed as part of the second approach described in [NIST SP 800-37, Rev. 2], The Risk Management Framework (RMF). The RMF predominantly operates at Level 3[56] – the operational level – and consists of seven process steps: Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor. Within the RMF, inputs from FARM at Level 1 and Level 2 are synthesized as part of the RMF Prepare step and then iteratively applied, tailored, and updated through each successive step of the RMF. Ultimately, Level 1 and Level 2 assumptions are iteratively customized and tailored to fit the specific operational level or procurement action context. For example, an enterprise may decide on strategic priorities and threats at Level 1 (enterprise level), which inform the criticality determination of mission and 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 Level 1 and Level 2 on a periodic basis.

Frame

Inputs and Preconditions

Frame is the step that establishes the context for C-SCRM at all three levels. The scope and structure of the enterprise supply chain, the overall risk management strategy, specific enterprise and mission and business process 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 enterprise and mission and business process level risk management strategies.

[56] The RMF does have some applications at Level 1 and Level 2, such as the identification of common controls.

These frameworks and methodologies provide bounds, standardization, and orientation for 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 enterprise's approach for managing risk." Enterprise-wide and C-SCRM risk-framing activities should iteratively inform one another. Assumptions that the enterprise makes about risk should flow down and inform risk framing within C-SCRM activities (e.g., enterprise's strategic priorities). As the enterprise's assumptions about cybersecurity risks throughout the supply chain 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:

- Enterprise policies, strategies, and governance
- Applicable laws and regulations
- Agency critical suppliers and contractual services
- Enterprise processes (security, quality, etc.)
- Enterprise 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 D-3 depicts the Frame step with its inputs and outputs along the three enterprise levels. At the enterprise level, activities will focus on framing conditions (i.e., assumptions, constraints, appetites and tolerances, and priorities and trade-offs) that are broadly applicable across the enterprise. The goal of framing is to contextualize cybersecurity risks throughout the supply chain in relation to the enterprise and its strategic goals and objectives. At Level 2, frame activities focus on tailoring the risk frame to individual mission and business processes (e.g., assumptions about service provider's role in achieving mission or business objectives).

Finally, at Level 3, conditions outlined at Level 1 and Level 2 iteratively inform each step of the RMF process. Beginning with the Prepare step, conditions outlined at Level 1 and Level 2 are used to establish the context and priorities for managing cybersecurity risks throughout the supply chain with respect to individual information systems, supplied system components, and system service providers. 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 bidirectional between levels as insights discovered while performing lower-level activities may update what is known about conditions outlined in higher levels.

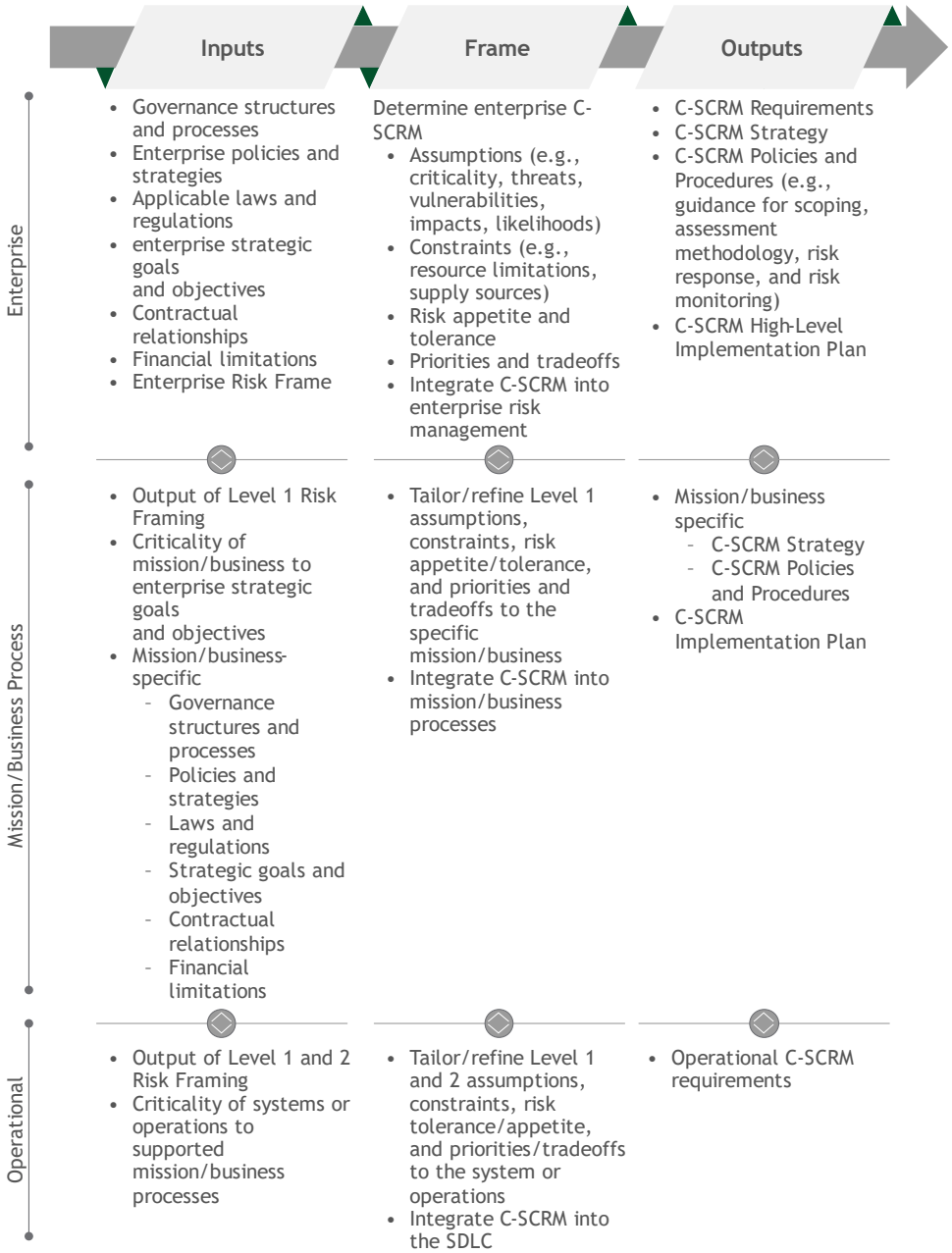

Fig. G-3: C-SCRM in the Frame Step

Figures G-3 through G-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. Inputs into the Frame step include inputs from other steps and from the enterprise risk management process that are shaping the C-SCRM process. Up-down arrows between the levels depict the 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 conditions, enterprises may find that Frame activities are performed relatively less often than the latter steps of the FARM process. Enterprises may re-perform Frame activities at defined intervals (e.g., annually, bi-annually) or based on defined triggers (e.g., 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 enterprise.

Supplemental Guidance

As a part of identifying risk assumptions within the broader Risk Management process (described in [NIST SP 800-39]), agencies should do the following:

- Develop an enterprise-wide C-SCRM policy.
- Identify which mission and business processes and related components are critical to the enterprise to determine the *criticality*.
- Define which mission and business processes and information systems compose the 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 levels, 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 the supply chain.
- Define C-SCRM mission, business, and operational-level requirements.
- Select appropriate assessment methodologies, depending on enterprise 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 supply chain to ensure that definitions remain current as evolutions occur over time.

These C-SCRM assumptions should be aligned as applicable to the broader 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 C-SCRM context at each successive risk management framework level. If and when new risk assumptions (i.e., Task 1-1) are identified, these should be provided as updates to any corresponding Enterprise Risk Assumptions (i.e., Enterprise Risk Management version of Task 1-1) as part of an iterative process.

Criticality

Critical processes are those that – 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 (e.g., hardware, software, and firmware). Mission-critical processes also depend on information and processes (performed by technology or people, to include support service contractors in some instances) that are used to execute the critical processes. Those components and processes that underpin and enable mission-critical processes or deliver defensive – and commonly shared – processes (e.g., access control, identity management, and crypto) and unmediated access (e.g., power supply) should also be considered critical. A criticality analysis is the primary method by which mission-critical processes, associated systems/components, and enabling infrastructure and support services are identified and prioritized. The criticality analysis also involves analyzing critical suppliers that may not be captured by internal criticality analysis (e.g., supply chain interdependencies including fourth- and fifth-party suppliers).

Enterprises will make criticality determinations as part of enterprise risk management activities based on the process outlined in [NISTIR 8179].[57] Where possible, C-SCRM should inherit those assumptions and tailor/refine them to include the C-SCRM context. In C-SCRM, criticality tailoring includes the initial criticality analysis of particular projects, products, and processes in the supply chain in relation to critical processes at each Level. For example, at Level 1, the enterprise may determine the criticality of holistic supplier relationships to the enterprise's overall strategic objectives. Then, at Level 2, the enterprise may assess the criticality of individual suppliers, products, and services to specific mission and business processes and strategic/operational objectives. Finally, at Level 3, the enterprise may assess the criticality of the supplied product or service to specific operational state objectives of the information systems.

Enterprises may begin by identifying key supplier-provided products or services that contribute to the operation and resiliency of enterprise processes and systems. Some of these elements may be captured or defined as part of disaster recovery continuity of operations plans. The criticality determination may be based on the role of each supplier, product, or service in achieving the required strategic or operational objective of the process or system. Requirements, architecture, and design inform the analysis and help identify the minimum set of supplier-provided products and/or services required for operations (i.e., at enterprise, mission and business process, and operational levels). The analysis combines top-down and bottom-up analysis approaches. The top-down approach in this model enables the enterprise to identify critical processes and then progressively narrow the analysis to critical systems that support those processes and critical components that support the critical functions of those systems. The bottom-up approach progressively traces the impact that a malfunctioning, compromised, or unavailable critical component would have on the system and, in turn, on the related mission and business process.

Enterprises that perform this analysis should include agency system and cybersecurity supply chain dependencies, to include critical fourth-party suppliers. For example, an enterprise may

[57] See NISTIR 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components*.

find exposures to cybersecurity risks that result from third-party suppliers receiving critical input or services from a common fourth-party supplier.

Determining criticality is an iterative process performed at all levels during both Frame and Assess. In Frame, criticality determination is expected to be performed at a high level using the available information with further detail incorporated through additional iterations or at the Assess step. Determining criticality may include the following:

- Define criticality analysis procedures to ensure that there is a set of documented procedures to guide the enterprise's criticality analysis across levels.
- Conduct enterprise and mission-level criticality analysis to identify and prioritize enterprise and mission objectives, goals, and requirements.
- Conduct operational-level criticality analysis (i.e., systems and sub-systems) 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 a detailed review (e.g., bottom-up analysis) of impacts and interactions between enterprise, mission, system/sub-systems, and components/sub-components to ensure cross-process interaction and collaboration.

Given the potential impact that a supply chain incident may have on an organization's operations, assets, and – in some instances – business partners or customers, it is important for organizations to ensure that in addition to criticality, materiality considerations are built into their supply chain risk management strategy, risk assessment practices, and overall governance of supply chain risks. In contrast to criticality, materiality considers whether the information would have been viewed by a reasonable investor making an investment decision as significantly altering the total mix of information available to the shareholder.[58] SEC guidance states:

> …the materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause. This includes harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities.

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 1) adversarial threats, such as cyber/physical attacks to the supply chain or to an information system component(s) traversing the supply chain; 2) accidental human errors; 3) structural failures, including the failure of equipment, environmental controls, and resource depletion; and 4) environmental threats, such as geopolitical disruptions,

[58] Refer to the glossary for definition details.

pandemics, economic upheavals, and natural or human-made disasters. With regard to adversarial threats, [NIST SP 800-39] states that enterprises should 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 and business process level), and at Level 3 (information system/services level), making explicit the types of threat sources to be addressed and the threat sources that are not addressed by the safeguards and 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 data. Threat information may come from multiple information sources, including the U.S. Intelligence Community (for federal agencies), DHS, CISA, the FBI, Information Sharing and Analysis Centers (ISAC), and open source reporting, such as news and trade publications, partners, suppliers, and customers. When applicable, enterprises may rely on the Federal Acquisition Security Council's (FASC) Information Sharing Agency (ISA) for supply chain threat information in addition to 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 enterprise's long-term assumptions about threat conditions based on its unique internal and external characteristics. During the Assess step, updated threat information is infused into the risk assessment to account for short-term variations in threat conditions (e.g., due to geopolitical circumstances) that would impact decisions made concerning the procurement of a product or service.

Information about the 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 supply chain. Supply chain cybersecurity threats are similar to information security threats, such as disasters, attackers, or industrial spies. Table G-1 lists examples of supply chain cybersecurity threat agents. Appendix G provides Risk Response Plans with examples of the Supply Chain Threat Sources and Agents listed in Table G-1.

Table G-1: Examples of Supply Chain Cybersecurity Threat Sources and Agents

Threat Sources	Threat	Examples
Adversarial: Counterfeiters	Counterfeits inserted into 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.[59]

[59] See [*Defense Industrial Base Assessment: Counterfeit Electronics*].

Threat Sources	Threat	Examples
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 4)	Foreign intelligence services seek to penetrate the supply chain and implant unwanted functionality (by inserting new or modifying existing functionality) into system to gather information or subvert[60] the system or mission operations when system is operational.
Adversarial: Terrorists	Unauthorized access	Terrorists seek to penetrate or disrupt the supply chain and may implant unwanted functionality to obtain information or cause physical disablement and destruction of systems through the supply chain.
Adversarial: Industrial Espionage/Cyber Criminals	Industrial Espionage or Intellectual Property Loss (see Appendix B, Scenario 2)	Industrial spies or cyber criminals seek ways to penetrate the supply chain to gather information or subvert system or mission operations (e.g., exploitation of an HVAC contractor to steal credit card information).
Adversarial: Organized Cyber Criminals	Ransomware leads to the disruption of a critical production process	Cyber-criminal organizations target enterprises with ransomware attacks in the hopes of securing ransom payments for monetary gain. Threat sources recognize that enterprises, especially manufacturers, have significant exposure to production disruptions.

[60] Examples of subverting operations include gaining unauthorized control to the cybersecurity supply chain or flooding it with unauthorized service requests to reduce or deny legitimate access.

Threat Sources	Threat	Examples
Systemic: Legal/Regulatory	Legal or regulatory complications impact the availability of key supplier-provided products and/or services	Weak anti-corruption laws, a lack of regulatory oversight, or weak intellectual property considerations, including threats that result from country-specific laws, policies, and practices intended to undermine competition and free market protections (e.g., the requirement to transfer technology and intellectual property to domestic providers in a foreign country).[61]
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. Other threats to the supply chain that result in economic risks include vulnerabilities to cost volatility, reliance on single-source suppliers, the cost to swap out suspect vendors, and resource constraints due to company size. [62]
Systemic Supply Disruptions	Production short-falls in rare earth metals lead to supply shortages for critical production inputs into semi-conductors	A variety of systemic and structural failures can cause supply shortage for products and product components, especially in cases where the source of supply is in a single geographical location.
Environmental: Disasters	Geopolitical or natural disaster led to supply chain disruption	The 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 fourth-party supplier.
Structural: Hardware Failure	Inadequate capacity planning leads to outage in a 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.

[61] Information and Communications Technology Supply Chain Risk Management Task Force: Threat Evaluation Working Group (v3), August 2021, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf. This report leveraged the 2015 version of the NIST SP 800-161.

[62] Information and Communications Technology Supply Chain Risk Management Task Force: Threat Evaluation Working Group (v3), August 2021, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf. This report leveraged the 2015 version of the NIST SP 800-161.

Threat Sources	Threat	Examples
Accidental: Negligent Insiders	Configuration error leads to data exposure	Employees and contractors with access to information systems are prone to errors that 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 G-2 provides examples of threat considerations and different methods for characterizing supply chain cybersecurity threats at different levels.

Table G-2: Supply Chain Cybersecurity Threat Considerations

Level	Threat Consideration	Methods
Level 1	• Enterprise business and mission • Strategic supplier relationships • Geographical considerations related to the extent of the enterprise's supply chain	• Establish common starting points for identifying supply chain cybersecurity threats. • Establish procedures for countering enterprise-wide threats, such as the insertion of counterfeits into critical systems and components.
Level 2	• Mission and business processes • Geographic locations • Types of suppliers (e.g., COTS, external service providers, or custom) • Technologies used enterprise-wide	• Identify additional sources of threat information specific to enterprise mission and business processes. • Identify potential threat sources based on the locations and suppliers identified through examining available agency cybersecurity supply chain information (e.g., from supply chain map). • Scope identified threat sources to the specific mission and business processes using agency the cybersecurity supply chain information. • Establish mission-specific preparatory procedures for countering threat adversaries and natural disasters.

Level	Threat Consideration	Methods
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 [NIST SP 800-53, Rev. 5]. 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 the services, systems, and components being developed and integrated (i.e., within the SDLC) as well as to the 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 enterprise's long-term assumptions about the their 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. Enterprises may make long-term supply chain cybersecurity vulnerability assumptions about:

- The entities within the supply chain itself (e.g., individual supplier relationships);
- The critical services provided through the supply chain that support the enterprise's critical mission and business processes;
- The products, systems, and components provided through the supply chain and used within the SDLC (i.e., being developed and integrated);
- The development and operational environment that directly impacts the SDLC; and
- The logistics and delivery environment that transports systems and components (logically or physically).

Vulnerabilities manifest differently across the three levels (i.e., enterprise, mission and business process, information system). At Level 1, vulnerabilities present as susceptibilities of the enterprise at large due to managerial and operating structures (e.g., policies, governance, processes), conditions in the supply chain (e.g., concentration of products or services from a single supplier), and characteristics of enterprise processes (e.g., use of a common system across critical processes). At Level 2, vulnerabilities are specific to a mission and business process and result from its operating structures and conditions, such as reliance on a specific system, supplier-provided input, or service to achieve specific mission and business process operating objectives. Level 2 vulnerabilities may vary widely across the different mission and business processes. Within Level 3, vulnerabilities manifest as deficiencies or weaknesses in a supplied product, the SDLC, system security procedures, internal controls, system implementations,

system inputs, or services provided through the supply chain (e.g., system components or services).

Enterprises should identify approaches to characterizing supply chain cybersecurity vulnerabilities that are consistent with the characterization of threat sources and events and with the overall approach employed by the enterprise for characterizing vulnerabilities. Vulnerabilities may be relevant to a single threat source or broadly applicable across threat sources (adversarial, structural, environmental, accidental). For example, a single point of failure in a network may be subject to disruptions caused by environmental threats (e.g., disasters) or adversarial threats (terrorists). Appendix B provides examples of supply chain cybersecurity threats, based on [NIST SP 800-30, Rev. 1, Appendix B].

All three levels should contribute to determining the enterprise's approach to characterizing vulnerabilities with progressively more detail identified and documented in the lower levels. Table G-3 provides examples of considerations and different methods for characterizing supply chain cybersecurity vulnerabilities at different levels.

Table G-3: Supply Chain Cybersecurity Vulnerability Considerations

Level	Vulnerability Consideration	Methods
Level 1	• Enterprise mission and business • Holistic supplier relationships (e.g., system integrators, COTS, external services) • Geographical considerations related to the extent of the enterprise's supply chain • Enterprise and Security Architecture • Criticality	• Examine agency cybersecurity supply chain information, including supply chain maps, to identify especially vulnerable entities, locations, or enterprises. • Analyze the agency mission for susceptibility to potential supply chain cybersecurity vulnerabilities. • Examine third-party provider and supplier relationships and interdependencies for susceptibility to potential supply chain cybersecurity vulnerabilities. • Review enterprise architecture and criticality to identify areas of weakness that require more robust cybersecurity supply chain considerations.
Level 2	• Mission and business processes • Geographic locations • Mission and 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.

Level	Vulnerability Consideration	Methods
		• 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[63] or other acceptable methodologies. • Consider using scoring guidance to prioritize vulnerabilities for remediation.
Level 3	• Individual technologies, solutions, and services • 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.

Impact and Harm

Impact is the effect on enterprise operations, enterprise assets, individuals, other enterprises, 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 enterprise's long-term assumptions about the effects that different cybersecurity events may 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) that may alter the impact's scope, duration, or magnitude is appropriately reflected in the analysis.

When possible, enterprises should inherit assumptions made by the enterprise on consequences and impact as part of enterprise risk management activities. For example, one of these activities is performing a business impact analysis (BIA) to determine or revalidate mission-critical and mission-enabling processes as part of the enterprise's continuity and emergency preparedness responsibilities. However, these assumptions may need to be developed if they do not yet exist. Enterprises may maintain impact or harm libraries that capture the enterprise's standing assumptions about the impact or harm of different cybersecurity event types (e.g., disclosure, disruption, destruction, modification) on the enterprise's assets. These libraries may break down impact and harm into individual impact types (e.g., operational, environmental, individual safety, reputational, regulatory/legal fines and penalties, IT recovery/replacement, direct financial damage to critical infrastructure sector).

[63] See https://nvd.nist.gov/.

For C-SCRM, enterprises should refine and update their consequences and impact assumptions to reflect the role that the availability, confidentiality, and integrity of supplier-provided products or services have on the enterprise's operations, assets, and individuals. For example, depending on its criticality, the loss of a key supplier-provided input or service may reduce the enterprise's operational capacity or completely inhibit its operations. In this publication, impact or harm is in relation to the enterprise's primary objectives and arises from products or services traversing the supply chain or 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 G-4 provides examples of how consequences and impact may be characterized at different levels of the enterprise.

Table G-4: Supply Chain Cybersecurity Consequence and Impact Considerations

Level	Impact Considerations	Methods
Level 1	• General enterprise-level impact assumptions • Supplier criticality (e.g., holistic supplier relationships)	• Examine the magnitude of exposure to individual entities within the supply chain. • Refine Level 2 analysis to determine aggregate Level 1 impacts on the enterprise's primary function resulting from cybersecurity events to and through the supply chain.
Level 2	• Process role in enterprise's primary function • Supplier criticality to mission/process (inputs and services)	For each type of cybersecurity event: • Refine Level 3 analysis to determine aggregate mission and business process impacts due to operational-level impacts from cybersecurity events to and through the supply chain. • Examine supplier network to identify business/mission-level impacts due to events that affect 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 system's 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 the supplier network to identify individual entities that may disrupt the availability of critical system inputs or services.

Enterprises 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 enterprises, supplier organizations, or applicable industry surveys. Where gaps in historical data exist, enterprises 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 enterprise. By interviewing well-positioned experts (e.g., technology or mission and business owners of assets), enterprises can tailor impact assumptions to reflect the enterprise'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 cybersecurity supply chain consequences and impacts:

- An earthquake in Malaysia reduces the amount of commodity dynamic random-access memory (DRAM) to 60 % of the world's supply, creating a shortage for hardware maintenance and new design.
- The accidental procurement of a counterfeit part results in premature component failure, thereby impacting the enterprise's mission performance.
- Disruption at a key cloud service provider results in operational downtime losses between $1.5 – $15 million 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 enterprise's enterprise risk management process and refined to account for C-SCRM-specific implications. However, the general assumptions may need to be developed if they do not yet exist. The likelihood analysis in the Frame step sets the enterprise's long-term assumptions about the relative likelihood of different adverse cybersecurity events. Likelihood is subject to extreme short-term variations based on point-in-time conditions (i.e., internal and external) and 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 1) adversary intent, 2) adversary capability, and 3) 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 which cybersecurity risks throughout the supply chain are probable to occur. Organizations may find historical data by looking to internal sources such as past incident trackers or external sources such as ISACs in order to approximate the likelihood of experiencing different cyber events. 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 forms and draw on similar techniques. To ensure that likelihood is appropriately contextualized for decision makers, enterprises should make time-bound likelihood estimates for cybersecurity events that affect the supply chain (e.g., likelihood within a given year).

Likelihood analysis will manifest differently across the three levels. Table G-5 captures some of the considerations and methods specific to each level.

Table G-5: Supply Chain Cybersecurity Likelihood Considerations

Level	Likelihood Consideration	Methods
Level 1	• General threat and likelihood assumptions for the enterprise • Level 2 and Level 3 likelihood findings • Overall engagement models with suppliers that alter opportunities for contact with threat sources	• Analyze critical national infrastructure implications that may increase the enterprise's target value. • Refine analyses from Level 2 and Level 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 and business process level conditions that 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 on by mission and business processes.
Level 3	• Enterprise system threat and likelihood assumptions • Supplier and system target value • Location and operating conditions • Supplier and system security policies, processes, and controls • Nature and degree of supplier contact with system (inputs, services)	• Analyze the nature of system inputs that come through the supply chain into the SDLC and that alter the likelihood of encountering threat sources. • Evaluate the system roles in Level 1 and Level 2 processes that alter the target value for potential adversaries. • Analyze supply chain characteristics (e.g., location of supplier) that may increase the likelihood that a system is affected by a threat source.

Agencies should identify which approaches they will use to determine the likelihood of a supply chain cybersecurity compromise, consistent with the overall approach used by the agency's risk management process. Agencies should ensure that appropriate procedures are in place to thoroughly document any risk analysis assumptions that lead to the tabulation of the final risk

exposure, especially in cases where high or critical impact risks are involved. Visibility into assumptions may be critical in enabling decision makers to take action.

RISK MANAGEMENT PROCESS CONSTRAINTS

TASK 1-2: Identify constraints[64] on the conduct of risk assessment, risk response, and risk monitoring activities within the enterprise.

Supplemental Guidance

Identify the following two types of constraints to ensure that the cybersecurity supply chain is integrated into the agency risk management process:

1. Agency constraints
2. Supply chain-specific constraints

Agency constraints serve as an overall input to framing the cybersecurity supply chain policy at Level 1, mission requirements at Level 2, and system-specific requirements at Level 3. Table G-6 lists the specific agency and cybersecurity supply chain constraints. Supply chain constraints, such as the C-SCRM policy and C-SCRM requirements, may need to be developed if they do not exist.

Table G-6: Supply Chain Constraints

Level	Agency Constraints	Supply Chain Constraints
Level 1	• Enterprise policies, strategies, and governance • Applicable laws and regulations • Mission and business processes • Enterprise processes (security, quality, etc.) • Resource limitations	• Enterprise C-SCRM policy based on the existing agency policies, strategies, and governance; applicable laws and regulations; mission and business processes; and enterprise 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 and business requirements that are incorporated into mission and business processes and enterprise architecture • Supplier service contracts, product warranties, and liability agreements

[64] Refer to [NIST SP 800-39], Section 3.1, Task 1-2 for a description of constraints in the risk management context.

Level	Agency Constraints	Supply Chain Constraints
Level 3	• Functional requirements • Security requirements	• Product and operational level C-SCRM capabilities • Supplier-provided system component warranties and service agreements

One the primary methods by which constraints are articulated is via a policy statement or directive. An enterprise's C-SCRM policy is a critical vehicle for directing C-SCRM activities. Driven by applicable laws and regulations, this policy should support enterprise policies, including acquisition and procurement, information security, quality, and supply chain and logistics. The C-SCRM policy should address the goals, objectives, and requirements articulated by the overall agency strategic plan, mid-level mission and business process strategy, and internal or external customers. The C-SCRM policy should also define the integration points for C-SCRM with the agency's Risk Management Process and SDLC.

C-SCRM policy should define the C-SCRM-related roles and responsibilities of the agency C-SCRM team and any dependencies or interactions among those roles. C-SCRM-related roles will articulate responsibilities for collecting supply chain cybersecurity 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 guidance on cybersecurity risks throughout the supply chain to engineering decisions that specify and select cyber products as the system design is finalized
- Procurement officer and maintenance engineer responsible for identifying and replacing defective hardware
- Delivery enterprise and acceptance engineers who verify that the system component is acceptable to receive into the acquiring enterprise
- 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
- The end user of cyber systems, components, and services

C-SCRM requirements should be guided by C-SCRM policies, mission and business processes, their criticality at Level 2, and known functional and security requirements at Level 3.

RISK APPETITE AND TOLERANCE

TASK 1-3: Identify the levels of risk appetite and tolerance across the enterprise.

Supplemental Guidance

On a broad level, risk appetite represents the types and amount of risk that an enterprise is willing to accept in pursuit of value [NISTIR 8286]. Conversely, risk tolerance is the enterprise or stakeholder's readiness to bear the remaining risk after a risk response in order to achieve their 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 that 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]. When establishing a risk management framework, it is recommended that enterprises establish risk appetite and risk tolerance statements that set risk thresholds. Then, where applicable, C-SCRM should align with risk appetite and tolerance statements from the enterprise risk management process. Once established, risk appetite and risk tolerance should be monitored and modified over time. For C-SCRM, these statements should be contextualized to inform decisions in the C-SCRM domain. Those responsible for C-SCRM across the enterprise should work with and support enterprise leaders on the development of C-SCRM-related risk appetite and risk tolerance statements. This should be done in accordance with criteria provided from the enterprise risk strategy (e.g., based on ERM risk categories).

Risk appetite and tolerance statements strongly influence the decisions made about C-SCRM across the three levels. Some enterprises may define risk appetite and risk tolerance as part of their broader enterprise risk management activities. In enterprises without a clearly defined risk appetite, Level 1 stakeholders should collaborate with enterprise leadership to define and articulate the enterprise's appetite for risk within the scope of the C-SCRM program's mandates. Enterprises with multiple organizations may choose to tailor risk appetite statements for specific organizations and mission and business processes. In general, risk appetite at Level 1 may be set to empower the enterprise to meet its value objectives (e.g., high appetite for supplier risk in support of reducing operating costs by 5 %). At Level 2 and Level 3, an organization's risk appetite statements are operationalized through risk tolerance statements. For example, an organization with a low appetite for supply chain cybersecurity risk may issue risk tolerance statements that necessitate restraint and control by Level 2 and Level 3 decision makers as they pursue strategic value (e.g., tolerance statement crafted based on strict production targets for an organization that supports a national security-related mission).

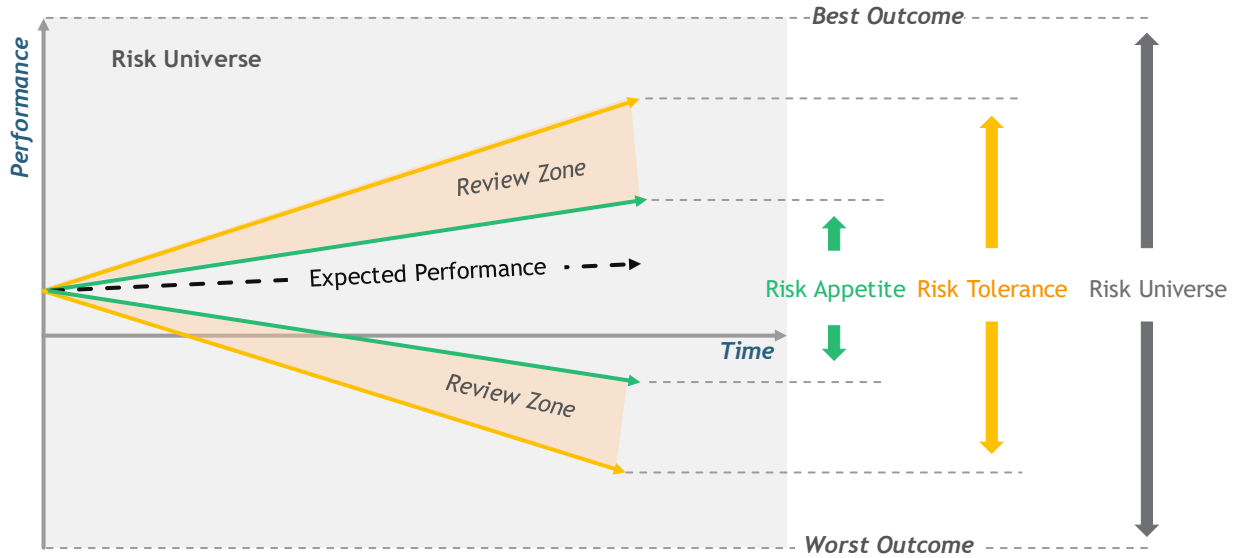

Fig. G-4: Risk Appetite and Risk Tolerance

Together, risk appetite and risk tolerance provide expectations and acceptable boundaries for performance against the organization's strategic objectives. Figure G-4 illustrates how risk appetite and risk tolerance may be used as guidelines for the organization's operational decision makers. Risk tolerance may be set with boundaries that exceed risk appetite to provide a degree of flexibility for achieving the organization's strategic objectives. However, operational decision makers should strive to remain within risk appetite during normal conditions and exceed the boundaries only as absolutely necessary (e.g., to capitalize on significant opportunities, avoid highly adverse conditions). Observed periods of performance in the *Review Zone,* which lies outside of risk appetite boundaries, should trigger a review of operational decisions and defined risk appetite and tolerance statements. The review is critical to ensuring that the organization's appetite for risk remains appropriate and applicable given the organization's internal and external operating conditions. For example, an organization operating during a global pandemic may find it necessary to take on additional levels of cyber risk exposure via alternative suppliers in order to circumvent supply shortages. Figure G-5 below provides an illustrative risk appetite and risk tolerance review process.

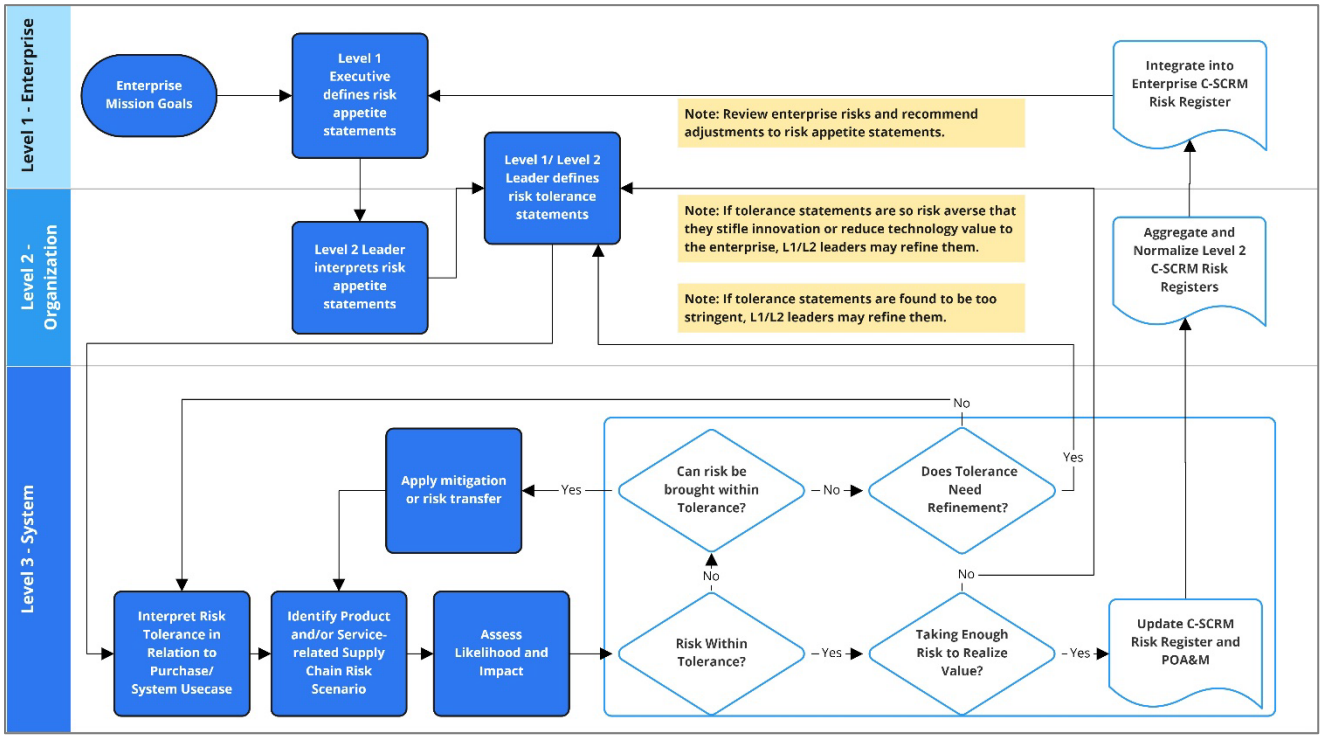

Fig. G-5: Risk Appetite and Risk Tolerance Review Process

In some cases, organizational leaders may find it necessary to rebalance guidance to avoid excess risk aversion behavior (i.e., performance below appetite) or excess risk-seeking behavior (i.e., performance above appetite) by decision makers.

Table G-7 shows additional examples of how risk appetite and risk tolerance statements work together to frame risk within an enterprise.

Table G-7: Supply Chain Risk Appetite and Risk Tolerance

Enterprise Constraints	Supply Chain Constraints
Low appetite for risk with respect to market objectives and requires 24/7 uptime	**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 %
Low appetite for risk with respect to production objectives that require > 99 % on-time delivery of products to customers with national security missions	**Near-zero tolerance** (i.e., no more than 5 % probability) for supply chain disruptions that cause production levels to fall below 99 % of target threshold for military products

Enterprise Constraints	Supply Chain Constraints
Low appetite for risk related to national security objectives that require 99 % effectiveness of security processes	**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
Moderate appetite for risk related to operational objectives of non-mission critical areas that require 99.5 % availability	**Moderate tolerance** (i.e., no more than 15 % probability) for system component failures causing non-critical system disruptions that exceed recovery time objectives by more than 10 %

To ensure that leadership has the appropriate information when making risk-based decisions, enterprises should establish measures (e.g., key performance indicators [KPIs], key risk indicators [KRIs]) to measure performance against defined risk appetite and risk tolerance statements. The identification of corresponding data sources for measurement should play a key role in the enterprise's defined processes for setting and refining risk appetite and tolerance statements. Risk appetite and risk tolerance should be treated as dynamic by the enterprise. This requires periodic updates and revisions based on internal (e.g., new leadership, strategy) and external (e.g., market, environmental) changes that impact the enterprise.

Enterprises should consider supply chain cybersecurity threats, vulnerabilities, constraints, and criticality when establishing, operationalizing, and maintaining the overall level of risk appetite and risk tolerance.[65]

PRIORITIES AND TRADE-OFFS

TASK 1-4: Identify priorities and trade-offs considered by the enterprise in managing risk.

Supplemental Guidance

Priorities and trade-offs are closely linked to the enterprise's risk appetite and tolerance statements, which communicate the amount of risk that is acceptable and tolerable to the enterprise in pursuit of its objectives. Priorities will take the form of long-term strategic objectives or near-term strategic imperatives that alter the risk decision calculus. From priorities and trade-offs, C-SCRM then receives critical strategic context required for Response step activities, such as Evaluation of Alternatives and Risk Response Decision. As a part of identifying priorities and trade-offs, enterprises should consider risk appetite, risk tolerance, supply chain cybersecurity threats, vulnerabilities, constraints, and criticality.

Priority and trade-off considerations will manifest different across the three levels. At Level 1, priority and trade-off considerations may favor existing supplier relationships in established

[65] The governance structures of federal departments and agencies 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 vice versa.

regions at the expense of new supplier cost advantages due to a desire to maintain confidence and stability. At Level 2, priority and trade-off considerations may favor centralized C-SCRM governance models that cover product teams in favor of greater security practice standardization. At Level 3, priorities and trade-offs may favor system components/sub-components that are produced in certain geographies in an effort to avoid environmental or geopolitical risks to the supply chain.

Outputs and Post Conditions

Within the scope of [NIST SP 800-39], the output of the risk framing step is the risk management strategy that identifies how enterprises intend to assess, respond to, and monitor risk over time. This strategy should clearly include any identified C-SCRM considerations and should result in the establishment of C-SCRM-specific processes throughout the agency. These processes should be documented in one of three ways:

1. Integrated into existing agency documentation,
2. Described in a separate set of documents that address C-SCRM, or
3. Utilizing a mix of separate and integrated documents based on agency needs and operations.

Regardless of how the outputs are documented, the following information should be provided as an output of the risk framing step:

- C-SCRM policy;
- Criticality, including prioritized mission and business processes and [FIPS 199] impact;
- Cybersecurity supply chain risk assessment methodology and guidance;
- Cybersecurity supply chain risk response guidance;
- Cybersecurity supply chain risk monitoring guidance;
- C-SCRM mission and business requirements;
- Revised mission and 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 enable prerequisites to effectively manage cybersecurity risks throughout the supply chain 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 are used to conduct a risk assessment. Numerous inputs (including criticality, risk appetite and tolerance, threats, vulnerability analysis, stakeholder knowledge, policy, constraints, and requirements) are combined and analyzed to gauge the likelihood and impact of a supply chain cybersecurity

compromise. Assess step activities are used to update the enterprise's long-term risk-framing assumptions to account for near-term variations and changes.

A cybersecurity supply chain risk assessment should be integrated into the overall enterprise risk assessment process. C-SCRM risk assessment results should be used and aggregated as appropriate to communicate potential or actual cybersecurity risks throughout the supply chain relevant to each risk management framework level. Figure G-6 depicts the Assess step with its inputs and outputs along the three levels.

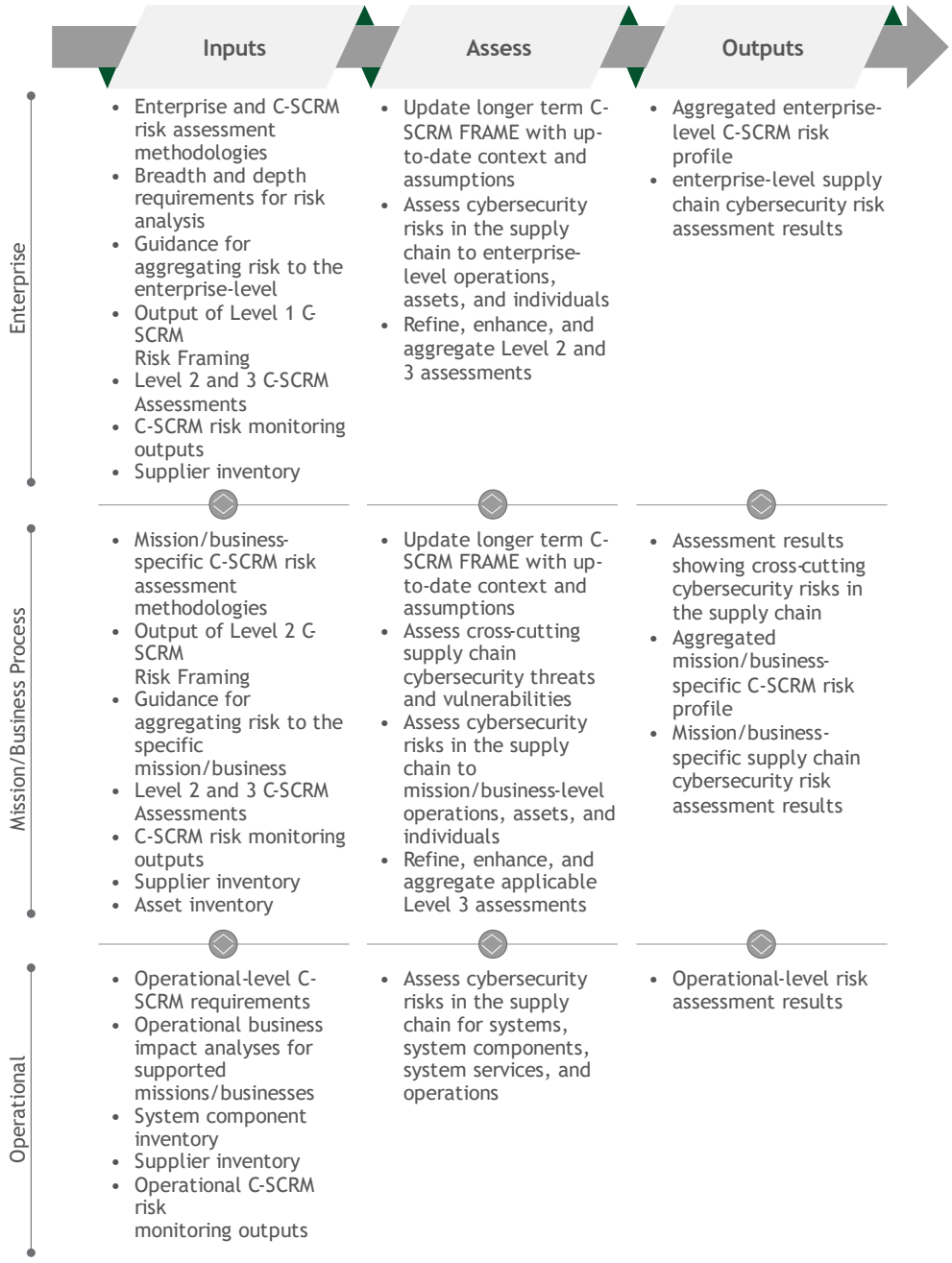

Fig. G-6: C-SCRM in the Assess Step[66]

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 that the assessment is scoped to minimally include relevant critical mission and business processes and to understand the relevance and impact of supply chain elements on these mission and business processes. As depicted in Figure G-5, vulnerability and threat analyses can then be performed in any order but should be performed iteratively to ensure that all applicable threats and

[66] More detailed information on the Risk Management Process can be found in Appendix C.

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

TASK 2-0: Update the 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 supply chain for the enterprise 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 that each entity has on mission priorities. The 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 the systems/components have been created.

Enterprises should update and tailor criticality established during the Frame step of the risk management process, including the [FIPS 199] system. For low-impact systems, enterprises should minimally assess criticality regarding interdependencies that systems may have with moderate or high-impact systems. If systems are used extensively throughout the enterprise, enterprises 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:

- Refining the dependency analysis and assessment to understand which components may require hardening given the system or network architecture;
- Obtaining and reviewing 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 the supply chain of these components;[67] and
- Updating information about the supply chain, historical data, and the SDLC to identify changes in critical supply chain paths and conditions.

The outcome of the updated criticality analysis is a narrowed, prioritized list of the enterprise's critical processes, systems, and system components, as well as a refined understanding of corresponding dependencies within the supply chain. Enterprises can use the criticality process in Task 1-1 to update their criticality analysis.

Because more information will be available in the Assess step, enterprises 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:

- Functional breakdown is an effective method for identifying processes and associated critical components and supporting defensive functions.
- Disaster recovery and continuity of operations plans often define critical systems and system components, which can be helpful in assigning criticality.
- Dependency analysis is used to identify the processes on which other critical processes depend (e.g., defensive functions, such as digital signatures used in software patch acceptance).
- The identification of all access points helps identify and limit unmediated access to critical functions and components (e.g., least-privilege implementation).
- Value chain analysis enables the understanding of inputs, process actors, outputs, and customers of services and products.
- 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 vulnerability analysis and threat analysis in determining the initial C-SCRM risk, as depicted in Figure D-4. 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 or 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 will likely be required to establish and maintain criticality analysis results. Enterprises should document or

[67] 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 that include 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.

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 enterprise 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], enterprises should conduct supply chain cybersecurity threat analysis and vulnerability analysis.

Threat Analysis

For C-SCRM, a threat analysis provides specific and timely characterizations of threat events (see Appendix C), potential threat actors (e.g., nation-state), and threat vectors (e.g., third-party supplier) to inform management, acquisition, engineering, and operational activities within an enterprise.[68] A variety of information can be used to assess potential threats, including open source, intelligence, and counterintelligence. Enterprises 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 the development and selection of appropriate mitigations to be applied in the Respond step. The focus of supply chain threat analysis should be based on the results of the criticality analysis.

Enterprises should use the information available from existing incident management activities to determine whether they have experienced a supply chain cybersecurity compromise and to further investigate such compromises. Agencies should define criteria for what constitutes a supply chain cybersecurity 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 enterprise to determine whether a supply chain compromise has occurred.

A supply chain cybersecurity threat analysis should capture at least the following data:

- An observation of cybersecurity supply chain-related attacks while they are occurring;
- Incident data collected post-cybersecurity supply chain-related compromise;
- An observation of tactics, techniques, and procedures used in specific attacks, whether observed or collected using audit mechanisms; and
- Natural and human-made disasters before, during, and after occurrence.

[68] Note that the threat characterization of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers may be benign.

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 [NIST SP 800-53, Rev. 5].

A vulnerability analysis is an iterative process that informs risk assessments and countermeasure selection. The vulnerability analysis works alongside the threat analysis to help inform the impact analysis and to help scope and prioritize the 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 supply chain cybersecurity vulnerabilities. Vulnerability analysis should begin by identifying vulnerabilities that are applicable to critical mission and business processes and the systems or 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 the vulnerability analysis may also identify additional threats or opportunities for threats that were not considered in earlier threat assessments.

Table G-8 provides examples of applicable supply chain cybersecurity vulnerabilities that can be observed within the three levels.

Table G-8: Examples of Supply Chain Cybersecurity Vulnerabilities Mapped to the Enterprise Levels

Level	Vulnerability Consideration	Methods
Level 1 – Enterprise	1) Deficiencies or weaknesses in enterprise governance structures or processes, such as the lack of a 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 enterprises as vulnerabilities. 2) Seek out alternative sources of new technology, including building in-house and leveraging trustworthy shared services and common solutions.
Level 2 – Mission and Business	1) No operational process in place for detecting counterfeits 2) No budget allocated for the implementation of a technical screening for acceptance testing of supplied system components entering the SDLC as replacement parts	1) Develop a program for detecting tainted or counterfeit products, and allocate an appropriate budget for resources and training. 2) Allocate a budget for acceptance testing (technical screening of components entering the SDLC).

	3) Susceptibility to adverse issues from innovative technology supply sources (e.g., technology owned or managed by third parties is buggy)	
Level 3 – Operation	1) Discrepancy in system functions not meeting requirements, resulting in substantial impact to performance	1) Initiate engineering changes to address functional discrepancy, and test corrections for performance impacts. Malicious alteration can happen to an agency system throughout the system life cycle. 2) Review vulnerabilities disclosed in the vulnerability disclosure report (VDR) published by software vendors.

RISK DETERMINATION

TASK 2-2: Determine the risk to enterprise operations and assets, individuals, other enterprises, and the Nation if identified threats exploit identified vulnerabilities.

Supplemental Guidance

Enterprises identify cybersecurity risks throughout the supply chain by considering the likelihood that known threats exploit known vulnerabilities to and through the supply chain, as well as the resulting consequences or adverse impacts (i.e., magnitude of harm) if such exploitations occur. Enterprises use threat and vulnerability information with likelihood and consequences/impact information to determine C-SCRM risk either qualitatively or quantitatively. Outputs from the Risk Determination at Level 1 and Level 2 should correspond directly with the RMF Prepare – Enterprise Level tasks described in [NIST 800-37, Rev. 2], while risk assessments completed for Level 3 should correspond 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 consideration of the characteristics of the threat sources, the identified vulnerabilities, and the enterprise's susceptibility to the supply chain cybersecurity compromise prior to and while the safeguards or 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 enterprise's mission. A cybersecurity supply chain risk assessment should consider two views:

1. The likelihood that one or more elements within the supply chain itself is compromised. This may impact, for example, the availability of quality components or increase the risk of intellectual property theft.
2. The likelihood of the system or component within the supply chain being compromised, for example, by malicious code inserted into a system or an electrical 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.

A likelihood determination should consider:

- Threat assumptions that articulate the types of threats that 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 enterprises
- Internal expert perspectives on the probability of a system 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 the probabilities of supply chain cybersecurity 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 capabilities, historical breach trends, or the frequency of breaches. The enterprise may use empirical data and statistical analysis to determine the specific probabilities of breach occurrence, depending on the type of data available and accessible within the enterprise.

Impact

Enterprises should begin impact analysis using methodologies and potential impact assumptions defined during the Frame step to determine the impact of a compromise and the impact of mitigating said compromise. Enterprises need to identify the various adverse impacts of compromise, including 1) the characteristics of the threat sources that could initiate the events, 2) identified vulnerabilities, and 3) the enterprise's susceptibility to such events based on planned or

implemented countermeasures. Impact analysis is an iterative process performed initially when a compromise occurs, when a mitigation approach is decided to evaluate the impact of change, and in the ever-changing SDLC when the situation or context of the system or environment changes.

Enterprises should use the results of an impact analysis to define an acceptable level of cybersecurity risks throughout the supply chain related to a specific system. Impact is derived from criticality, threat, and vulnerability analysis results and should be based on the magnitude of effect on enterprise operations, enterprise assets, individuals, other enterprises, 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 risk-based decisions and whether to accept, avoid, mitigate, or share the resulting risks and the consequences of such decisions.

Enterprises should document the overall results of assessments of cybersecurity risk throughout the supply chain in risk assessment reports.[69] Cybersecurity supply chain risk assessment reports should cover risks in all three enterprise levels, as applicable. Based on the enterprise structure and size, multiple assessment reports on cybersecurity risks throughout the supply chain may be required. Agencies are encouraged to develop individual reports at Level 1. For Level 2, agencies should integrate cybersecurity risks throughout the supply chain into the respective mission-level business impact analysis (BIA) and may want to develop separate mission-level assessment reports on cybersecurity risks throughout the supply chain. For Level 3, agencies may want to integrate cybersecurity risks throughout the supply chain 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

Enterprises may use risk aggregation to combine several discrete or lower-level risks into a more general or higher-level risk [NIST SP 800-30, Rev. 1]. Risk aggregation is especially important for C-SCRM as enterprises strive to understand their risk exposure to the supply chain in contrast to assets at different levels of the organization. Ultimately, enterprises may wish to aggregate and normalize their C-SCRM risk assessment results with other enterprise risk assessments to develop an understanding of their total risk exposure across risk types (e.g., financial, operational, legal/regulatory). This aggregation may occur at an enterprise level in cases where the enterprise consists of multiple subordinate enterprises. Each subordinate enterprise would combine and normalize risks within a single enterprise risk register. Risk aggregation may also occur from Level 2 mission and business process level registers into a single Level 1 enterprise-level risk register. To ease this process, enterprises 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), enterprises can more easily develop a holistic understanding of aggregate Level 1 and Level 2 risk exposures. In many cases, however,

[69] See [NIST SP 800-30, Rev. 1] Appendix K for a description of risk assessment reports.

enterprises will find that risk assessments completed at lower levels contain overlapping estimates for likelihood and impact magnitude. In these cases, the sum of the pieces (i.e., risk exposure ratings at lower levels) are greater than the whole (i.e., aggregate risk exposure of the enterprise). To overcome these challenges, enterprises can employ a variety of techniques. Enterprises 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, enterprises should ensure that assessments of risk produce discrete outputs by adopting mutually exclusive and collectively exhaustive (MECE) frameworks. MECE frameworks guide the analysis of inputs (e.g., threats, vulnerabilities, impacts) and allow the enterprise to minimize overlapping assumptions and estimates. Instead of summing risks from lower levels together, enterprises may elect to perform a new holistic assessment at an upper level that leverages the combined assessment results from lower levels. Doing so can help enterprises avoid double-counting risks, resulting in an overestimation of their aggregate risk exposure. Enterprises 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), enterprises 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,
- The establishment of relationships between the critical aspects of the system's supply chain infrastructure (e.g., SDLC) and applicable threats and vulnerabilities,
- Understanding of the likelihood and impact of a potential supply chain cybersecurity compromise,
- Understanding mission and system-specific risks,
- Documented assessments of cybersecurity risks throughout the supply chain related to mission and business processes or individual systems, and
- The integration of results of relevant assessments of cybersecurity risks throughout supply chain into the enterprise risk management process.

Respond

Inputs and Preconditions

Respond is the step in which the individuals conducting the 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 an appropriate manner to inform and guide risk-based decisions. This will allow decision makers to finalize appropriate risk responses based on the set of options and the corresponding risk factors of choosing the various options. Sometimes, an appropriate response

is to simply monitor the adversary's activities and behavior to better understand the tactics and activities.

Cybersecurity supply chain risk response should be integrated into the overall enterprise risk response. Figure G-6 depicts the Respond step with its inputs and outputs along the three enterprise levels.

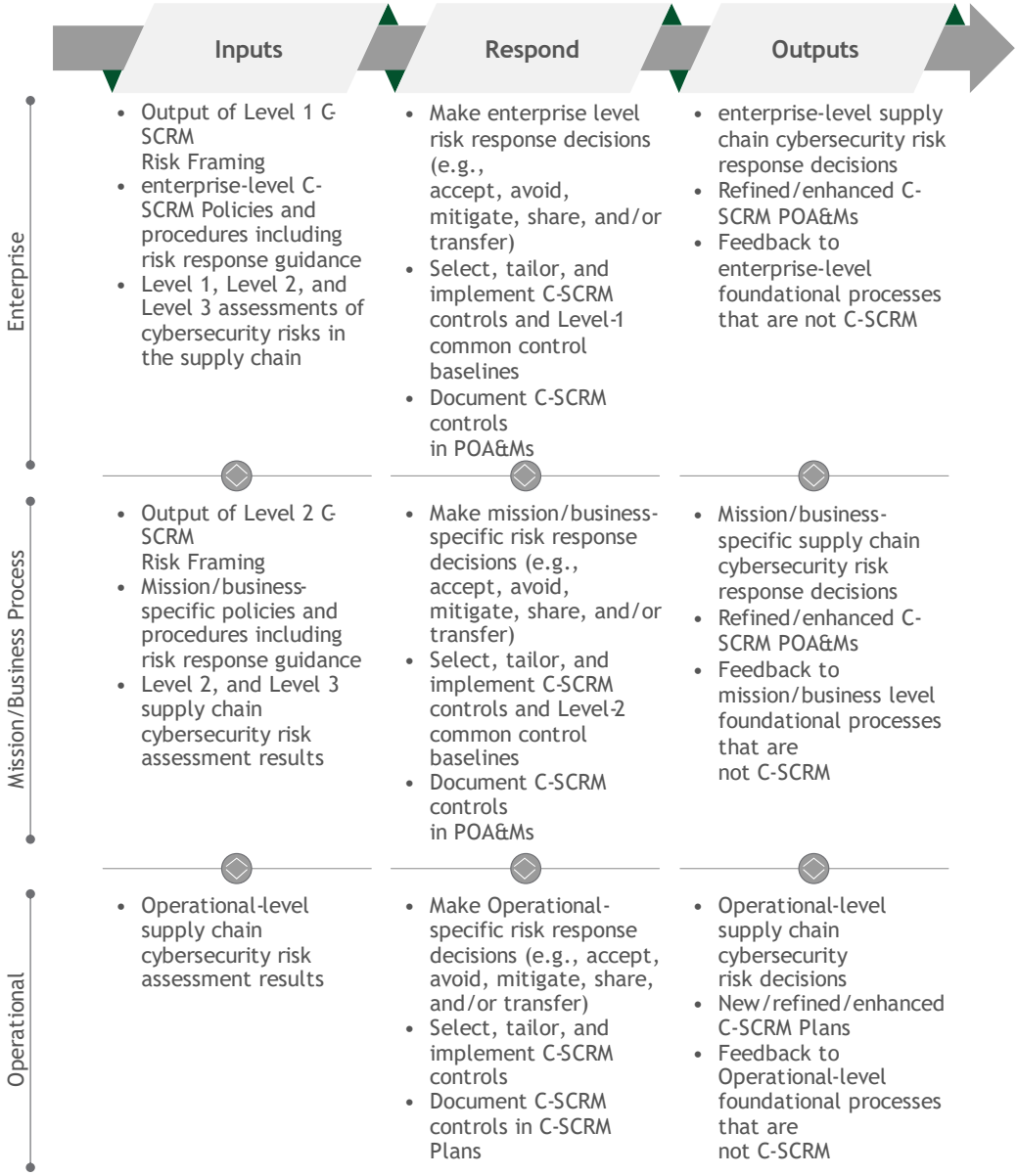

Fig. G-7: C-SCRM in the Respond Step[70]

[70] More detailed information on the Risk Management Process can be found in Appendix C.

Activities

RISK RESPONSE IDENTIFICATION

TASK 3-1: Identify alternative courses of action to respond to risks identified during the risk assessment.

Enterprise's risk response strategies will be informed by risk management strategies developed for the enterprise (i.e., Level 1) and mission and business processes (i.e., Level 2). Risk response strategies will include general courses of action that the enterprise may take as part of its risk response efforts (e.g., accept, avoid, mitigate, transfer or share). As part of mitigation efforts, enterprises 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 the 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 into agreements made with third-party providers. These controls are included because they apply to C-SCRM.

This process should begin by determining acceptable risks 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 enterprise to achieve its defined risk threshold. An evaluation of alternatives typically occurs at Level 1 or Level 2 with a focus on anticipated enterprise-wide impacts of C-SCRM on the enterprise's ability to successfully carry out enterprise missions and processes. When carried out at Level 3, an evaluation of alternatives focuses on the SDLC or the amount of time available for implementing the course of action.

Each course of action analyzed may include a combination of risk acceptance, avoidance, mitigation, transfer, and sharing. For example, an enterprise may elect to share a portion of its risk with a strategic supplier through the selection of controls included under contractual terms. Alternatively, an enterprise may choose to mitigate risks to acceptable levels through the selection and implementation of controls. In many cases, risk strategies will leverage a combination of risk response courses of action.

During the evaluation of alternatives, the enterprise will analyze available risk response courses of action for identified cybersecurity risks throughout the supply chain. The goal of this exercise is to enable the enterprise to achieve an appropriate balance between C-SCRM and the functionality needs of the enterprise. As a first step, enterprises should ensure that risk appetites and tolerances, priorities, trade-offs, applicable requirements, and constraints are reviewed with stakeholders who are familiar with the broader enterprise requirements, such as cost, schedule, performance, policy, and compliance. Through this process, the enterprise will identify risk

response implications to the enterprise's broader requirements. Equipped with a holistic understanding of risk response implications, enterprises 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 enterprise levels and SDLC processes. For example, C-SCRM controls may range from using a blind buying strategy to the obscure end use of a critical component and design attributes (e.g., input validation, sandboxes, and anti-tamper design). For each implemented control, the enterprise should identify someone who will be 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 enterprise may be unknowingly trading one risk for a larger risk 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], enterprises should select, tailor, and finalize C-SCRM controls based on an evaluation of alternatives and an overall understanding of threats, risks, and supply chain priorities. Within Level 1 and Level 2, the resulting decision and the selected and tailored common control baselines (i.e., revisions to established baselines) should be documented within a C-SCRM-specific Risk Response Framework.[71] Within Level 3, the resulting decision and 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 enterprise. 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 enterprise's risk executives, mission owners, and system owners, as appropriate. Risk response decisions are heavily influenced by the enterprise's predetermined appetite and tolerance for risk. Using robust risk appetite and tolerance definitions, decision makers can ensure consistent alignment of the enterprise's risk decisions with its strategic imperatives. Robust definitions of risk appetite and tolerance may also enable enterprises to delegate risk decision responsibility to lower levels of the enterprise and provide greater autonomy across all levels.

Within Level 1 and Level 2, the resulting decisions should be documented with any changes to requirements or selected common control baselines (i.e., enterprise or mission and business

[71] More information Risk Response Frameworks and explicit examples can be found on in Appendix B.

process 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:

- A description of the threat source, threat event, exploited vulnerability, and threat event outcome;
- An analysis of the likelihood and impact of the risk and final risk exposure;
- A description of 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 and 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 supply chain cybersecurity compromise. Ultimately, the C-SCRM plan should cover the full SDLC, document a C-SCRM baseline, and identify cybersecurity 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 cybersecurity supply chain monitoring.

C-SCRM plans should:

- Summarize the environment as determined in the Frame step, such as applicable policies, processes, and procedures based on enterprise and mission requirements currently implemented in the enterprise
- 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 the Respond step)
- Provide tailoring decisions for selected controls, including the rationale for the decision
- Describe feedback processes among the levels to ensure that cybersecurity 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 the implementation of the C-SCRM plan and assess the effectiveness of the implementation[72]
- Define a frequency for reviewing and revising the plan
- Include criteria that would trigger revision, such as life cycle milestones, gate reviews, or significant contracting activities

[72] NIST SP 800-55, Rev. 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.

- Include suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers in C-SCRM plans if they are 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 the 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 when developing and revising the requirements and controls applied at the higher levels. C-SCRM plans should be interconnected and reference each other when appropriate.

Table G-9 summarizes the controls to be contained in Risk Response Frameworks at Level 1 and Level 2, the C-SCRM plans at Level 3, and examples of those controls.

Table G-9: Controls at Levels 1, 2, and 3

Level	Controls	Examples
Level 1	Provides enterprise common control baselines to Level 2 and Level 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 supplier, developer, system integrator, external system service provider, and other ICT/OT-related service provider information • Cybersecurity supply chain training and awareness for acquirer staff at the enterprise level
Level 2	• Inherits common controls from Level 1 • Provides mission and business process-level 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 to 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	Controls	Examples
Level 3	• Inherits common controls from Level 1 and Level 2 • Provides system-specific controls for Level 3 • Provides feedback to Level 1 and Level 2 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 the supply chain (e.g., as testing or integrated development environments) • System-specific cybersecurity 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 that enterprises should include in their C-SCRM planning activities.

RISK RESPONSE IMPLEMENTATION

TASK 3-4: Implement the course of action selected to respond to risk.

Enterprises 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 agreements with third-party providers. These requirements and resulting controls will be incorporated into the SDLC and other enterprise 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 enterprises 1) verify compliance, 2) determine the ongoing effectiveness of risk response measures, and 3) identify risk-impacting changes to enterprise information systems and environments of operation.

Changes to the enterprise, mission and business processes, operations, or the supply chain can directly impact the enterprise's cybersecurity supply chain. The Monitor step provides a mechanism for tracking such changes and ensuring that they are appropriately assessed for

impact (in the Assess step). If the cybersecurity supply chain is redefined as a result of monitoring, enterprises should coordinate with their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to resolve implications and mutual obligations. A critical component of the Monitor step includes the upward dissemination of information to inform higher level risk assessments (e.g., mission and business process assessment informs enterprise assessment). This ensures that enterprise leaders maintain visibility into risk conditions across the enterprise.

Enterprises should monitor for supply chain risk events to reassess risk and determine appropriate risk responses. This should include determining whether the event has triggered an incident or compels the need for information sharing. Examples of supply chain risk events include:

- Change of ownership, merger, or acquisition
- Disruption to the supply chain
- Continuity or emergency event that affects a source or its supply chain
- Ransomware or other cybersecurity attack that affects a source or its supply chain
- New information about a critical vulnerability that may or does affect technology used by the source and/or its supply chain
- Discovery of a counterfeit or non-conforming product or component
- Change in location for manufacturing or software development, especially changes from domestic to foreign locations
- OEM no longer produces and/or supports a product or critical component of a product
- Evidence of non-disclosed functionality or features of a covered article
- Any notification that requires additional investigation to determine whether the confidentiality, integrity, and availability of the Federal Government's data and information systems can be directly attributed to an attack involving the refurbishment, tampering, and counterfeiting of ICT products
- Presence of covered articles produced by a prohibited or otherwise non-authorized source
- Evidence of suspicious Foreign Ownership, Control, or Influence (FOCI)
- Other changes that may negatively affect the risk profile of the source, the covered article, and/or the associated supply chain (e.g., loss of key personnel, degradation of the company's financial health, etc.)

Enterprises should integrate C-SCRM into existing continuous monitoring programs.[73] In the event that a continuous monitoring program does not exist, C-SCRM can serve as a catalyst for establishing a comprehensive continuous monitoring program. Figure G-7 depicts the Monitor step with inputs and outputs along the three enterprise levels.

[73] 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.

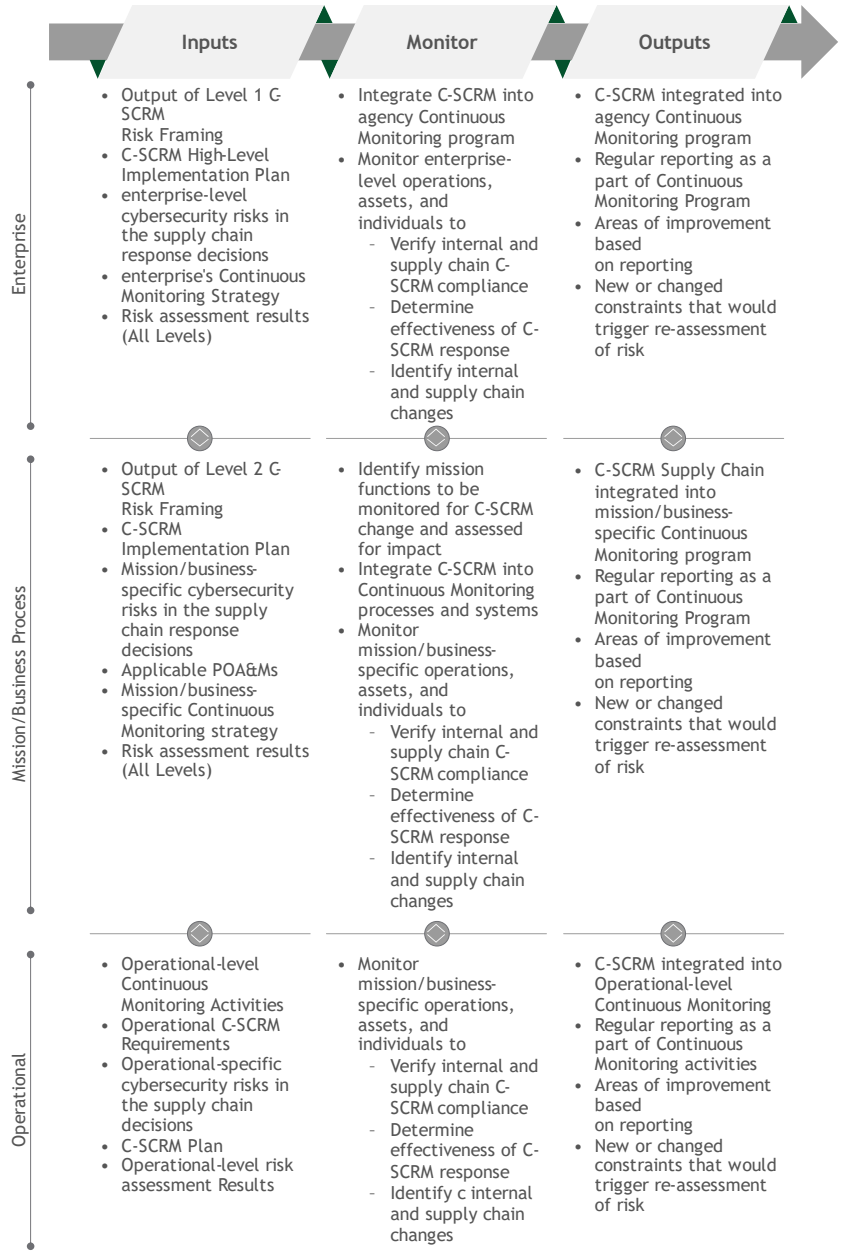

Fig. G-8: C-SCRM in the Monitor Step[74]

Activities

RISK MONITORING STRATEGY

TASK 4-1: Develop a risk monitoring strategy for the enterprise that includes the purpose, type, and frequency of monitoring activities.

[74] More detailed information on the Risk Management Process can be found in Appendix C.

Supplemental Guidance

Enterprises should integrate C-SCRM considerations into their overall risk monitoring strategy. Monitoring cybersecurity risks throughout the supply chain may require access to information that agencies may not have traditionally collected. Some of the information will need to be gathered from outside of the agency, such as from open sources, suppliers, or 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 assumptions about the 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;
- 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.

Enterprises 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 cybersecurity risks throughout the supply chain.

RISK MONITORING

TASK 4-2: Monitor enterprise information systems and environments of operation on an ongoing basis to verify compliance, determine the effectiveness of risk response measures, and identify changes.

According to [NIST SP 800-39], enterprises should monitor compliance, effectiveness, and change. Monitoring compliance within the context of C-SCRM involves monitoring an enterprise'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 the 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 cybersecurity risks throughout the supply chain.

To monitor for changes, enterprises should establish regular intervals at which they review suppliers and their supplied products and services. The reassessment intervals should be determined as needed and appropriate for the enterprise. Enterprises also need to identify and document a set of off-cycle triggers that would signal an alteration to the state of cybersecurity risks throughout the supply chain. While the categories of triggers will likely include changes to constraints as identified in Table D-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 enterprises.

An example of a cybersecurity supply chain change is two key vetted suppliers[75] 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, a potential deficit of components may result from an insufficient supply of components. If none of the remaining suppliers are vetted, this deficit may result in the uncertain integrity of the remaining components. If the enterprise policy directs the use of vetted components, this event may result in the enterprise's inability to fulfill its mission needs. Supply chain change may also arise as a result of a company experiencing a change in ownership. A change in ownership could have significant implications, especially in cases where the change involves a transfer of ownership to individuals who are citizens of a different country from that of the original owners.

In addition to regularly updating existing risk assessments at all levels of the enterprise with the results of ongoing monitoring, the enterprise should determine the triggers of a reassessment. Some triggers may include the availability of resources, changes to cybersecurity risks throughout the supply chain, natural disasters, or mission collapse.

In order for monitoring to be effective, the state of cybersecurity supply chain risk management needs to be communicated to decision makers across the enterprise in the form of C-SCRM reporting. Reporting should be tailored to meet the specific needs of its intended audience. For example, reporting to Level 1 decision makers may summarize the C-SCRM implementation coverage, efficiency, effectiveness, and overall levels of exposure to cybersecurity risks throughout the supply chain at aggregate levels across the enterprise. Where applicable and appropriate for the audience, reporting may focus on specific areas in Level 2 and Level 3 that require executive leadership attention. To aid in tailoring reporting, reporting requirements should be defined in collaboration with the intended audience and updated periodically to ensure that it remains efficient and effective.

Outputs and Post Conditions

Enterprises should integrate the cybersecurity 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.

[75] A vetted supplier is one with whom the organization is comfortable doing business. This level of comfort is usually achieved through the development of an organization-defined set of supply chain criteria and then *vetting* suppliers against those criteria.

APPENDIX H: GLOSSARY

Term	Definition
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 by the organization.
acquirer [ISO/IEC/IEEE 15288, adapted]	Organization or entity that acquires or procures a product or service.
acquisition [NIST SP 800-64, adapted]	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.
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 boundary [NIST SP 800-53 Rev. 5]	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.
authorizing official [NIST SP 800-53 Rev. 5]	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.
authorization to operate [NIST SP 800-53 Rev. 5]	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.
baseline [CNSSI 4009]	Hardware, software, databases, and relevant documentation for an information system at a given point in time.
C-SCRM control	A safeguard or countermeasures prescribed for the purpose of reducing or eliminating the likelihood and/or impact/consequences of cybersecurity risks throughout the supply chain.

Term	Definition
cybersecurity compromise in the supply chain	A cybersecurity incident in the supply chain (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 supply chain incident can occur anywhere during the life cycle of the system, product or service.
cybersecurity risks throughout the supply chain	The potential for harm or compromise arising from suppliers, their supply chains, their products, or their services. Cybersecurity risks throughout the supply chain 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.
cybersecurity supply chain risk assessment	A systematic examination of cybersecurity risks throughout the supply chain, likelihoods of their occurrence, and potential impacts.
cybersecurity supply chain risk management	A systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures. *Note:* For the purposes of NIST publications SCRM and C-SCRM refer to the same concept. This is because NIST is addressing only the cybersecurity aspects of SCRM. Other organizations may use a different definition of SCRM which is outside the scope of this publication. This publication does not address many of the non-cybersecurity aspects of SCRM.
defense-in-breadth [NIST SP 800-53 Rev. 5]	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.
degradation	A decline in quality or performance; the process by which the decline is brought about.
developer [NIST SP 800-53 Rev. 5, adapted]	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.

Term	Definition
element	See *supply chain element*.
enhanced overlay	An overlay that adds processes, controls, enhancements, and additional implementation guidance specific to the purpose of the overlay.
exposure [ISO Guide 73, adapted]	Extent to which an organization and/or stakeholder is subject to a risk
external system service [NIST SP 800-53 Rev. 5]	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.
external system service provider [NIST SP 800-53 Rev. 5]	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.
fit for purpose [ITIL Service Strategy, adapted]	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.
ICT/OT-related service providers	Any organization or individual providing services which may include authorized access to an ICT or OT system
impact [NIST SP 800-53 Rev. 5]	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.
Information and Communications Technology [ISO/IEC 2382, adapted]	Encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information.
information system [NIST SP 800-53 Rev. 5]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
life cycle [ISO/IEC/IEEE 15288, adapted]	Evolution of a system, product, service, project, or other human-made entity.

Term	Definition
likelihood [ISO/IEC 27000]	Chance of something happening.
materiality 1) U.S. Supreme Court in TSC Industries v. Northway, 426 U.S. 438, 449 (1976) 2) Commission Statement and Guidance on Public Company Cybersecurity Disclosures), SECURITIES AND EXCHANGE COMMISSION 17 CFR Parts 229 and 249 [Release Nos. 33-10459; 34-82746]	1) The standard of materiality articulated by the U.S. Supreme Court in TSC Industries v. Northway, 426 U.S. 438, 449 (1976) (a fact is material "if there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision or if it "would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available" to the shareholder). 2) The materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations. The materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause. This includes harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities.
organizational user [NIST SP 800-53 Rev. 5, adapted]	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.
overlay [NIST SP 800-53 Rev. 5]	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.

Term	Definition
pedigree	The validation of the 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.
program manager	See *system owner*.
provenance [NIST SP 800-53 Rev. 5]	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.
residual risk [NIST SP 800-16, adapted]	Portion of risk remaining after controls/countermeasures have been applied.
risk [NIST SP 800-39]	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.
risk appetite [NISTIR 8286]	The types and amount of risk, on a broad level, [an organization] is willing to accept in its pursuit of value.
risk framing [NIST SP 800-39]	The set of assumptions, constraints, risk tolerances, and priorities/trade-offs that shape an organization's approach for managing risk.
risk management [NIST SP 800-53 Rev. 5]	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.
risk mitigation [NIST SP 800-53 Rev. 5]	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Term	Definition
risk response [NIST SP 800-53 Rev. 5, adapted]	Intentional and informed decision and actions to accept, avoid, mitigate, share, or transfer an identified risk.
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 [NIST 8286, adapted]	The organization's or stakeholder's readiness to bear the remaining risk after responding to or considering the risk in order to achieve its objectives.
secondary market	An unofficial, unauthorized, or unintended distribution channel.
security control [NIST SP 800-53 Rev. 5]	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.
software bill of materials Exec. Order No. 14028, supra note 1, § 10(j)	A formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product.
supplier [ISO/IEC/IEEE 15288, adapted] [NIST SP 800-53 Rev. 5, adapted from definition of "developer"]	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.
supply chain [ISO 28001, adapted]	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.
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.

Term	Definition
supply chain risk information [FASCA]	Includes, but is not limited to, information that describes or identifies: (1) Functionality of covered articles, including access to data and information system privileges; (2) Information on the user environment where a covered article is used or installed; (3) The ability of the source to produce and deliver covered articles as expected (i.e., supply chain assurance); (4) 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); (5) Implications to national security, homeland security, and/or national critical functions associated with use of the covered source; (6) Vulnerability of federal systems, programs, or facilities; (7) Market alternatives to the covered source; (8) 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; (9) Likelihood of a potential impact or harm, or the exploitability of a system; (10) Security, authenticity, and integrity of covered articles and their supply and compilation chain; (11) Capacity to mitigate risks identified; (12) Credibility of and confidence in other supply chain risk information; (13) Any other information that would factor into an analysis of the security, integrity, resilience, quality, trustworthiness, or authenticity of covered articles or sources; (14) A summary of the above information and, any other information determined to be relevant to the determination of supply chain risk.
system [NIST SP 800-53 Rev. 5, adapted]	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.

Term	Definition
	Note 3: System-of-systems is included in the definition of system.
system assurance [NDIA]	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.
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 [NIST SP 800-34 Rev. 1, adapted]	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal.
system integrator	Those organizations that provide customized services to the acquirer including for example, custom development, test, operations, and maintenance.
system owner (or program manager) [NIST SP 800-53 Rev. 5]	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of a system.
threat [NIST SP 800-53 Rev. 5]	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.
threat analysis	See *threat assessment*.
threat assessment [NIST SP 800-53 Rev. 5, adapted]	Formal description and evaluation of threat to a system or organization.
threat event [NIST SP 800-30 Rev. 1]	An event or situation that has the potential for causing undesirable consequences or impact.
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.

Term	Definition
threat scenario [NIST SP 800-30 Rev. 1]	A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time.
threat source [NIST SP 800-53 Rev. 5]	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.
transparency	See *visibility*.
trust [SwA]	The confidence one element has in another, that the second element will behave as expected.
trustworthiness [NIST SP 800-53 Rev. 5, adapted]	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.
validation [ISO 9000]	Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled. *Note:* The requirements were met.
verification [CNSSI 4009] [ISO 9000, adapted]	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled. *Note:* The intended output is correct.
visibility [ISO/IEC 27036, adapted]	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.
vulnerability [NIST SP 800-53 Rev. 5]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
vulnerability assessment [NIST SP 800-53 Rev. 5, adapted]	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.

APPENDIX I: 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**
CISS	**Cyber Incident Severity Schema**
CLO	**Chief Legal Officer**
COO	**Chief Operating Officer**
CPO	**Chief Privacy Officer**
CRO	**Chief Risk Officer**
CSO	**Chief Security 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	**Cybersecurity Supply Chain Risk Management**
CSF	**Cybersecurity Framework**
CTO	**Chief Technology Officer**
CUI	**Controlled Unclassified Information**
CVE	**Common Vulnerability Enumeration**
CVSS	**Common Vulnerability Scoring System**
CWE	**Common Weakness Enumeration**
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**
SBOM	**Software Bill of Materials**
SCIF	**Sensitive Compartmented Information Facility**
SCRI	**Supply Chain Risk Information**
SCRM	**Supply Chain Risk Management**
SCRSS	**Supply Chain Risk Severity Schema**
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**
VDR	**Vulnerability Disclosure Report**

APPENDIX J: RESOURCES

RELATIONSHIP TO OTHER PROGRAMS AND PUBLICATIONS

This 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 enterprise-wide activities, as well as a series of legislative developments following its initial release. These resources are complementary and help enterprises 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.

NIST Publications

This document 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 and scoping C-SCRM activities to high-impact components or systems [FIPS 199]
- NIST SP 800-30, Rev. 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, Rev. 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, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations,* to provide information security controls for enhancing and tailoring to the C-SCRM context [NIST SP 800-53, Rev. 5]
- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, to codify control baselines and C-SCRM supplementary guidance and [NIST SP 800-53B]
- NIST SP 800-150, *Guide to Cyber Threat Information Sharing*, to provide guidelines for establishing and participating in cyber threat information relationships [NIST SP 800-150]
- NIST SP 800-160 Vol. 1, *Systems Security Engineering* [NIST SP 800-160 Vol. 1] and NIST SP 800-160 Vol. 2, Rev. 1, *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 800-171, Rev. 2, *Protecting Controlled Information in Nonfederal Systems and Organizations*, for recommended security requirements to protect the confidentiality of CUI [NIST SP 800-171, Rev. 2]
- NIST SP 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information – A Supplement to NIST Special Publication 800-171*, for

recommended enhanced security requirements for protecting the confidentiality of CUI [NIST SP 800-172]
- NIST SP 800-181, Rev. 1, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, as a means of forming a common lexicon for 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 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*, to elucidate recent C-SCRM trends in the private sector [NISTIR 8276]
- 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]

Regulatory and Legislative Guidance

This document is heavily informed by regulatory and legislative guidance, including:

- Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control*
- Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*
- 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*
- Public Law 115–232 § 889, *Prohibition on Contracting Certain Telecommunications and Video Surveillance Services or Equipment*
- Federal Register, Vol. 84, No. 156, *Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment*, August 13, 2019
- FAR Part 4, Subpart 4.20, *Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab*
- (GAO), *Challenges and Policy Considerations Regarding Offshoring and Foreign Investment Risks*, September 2019
- Executive Order 14028, *Improving the Nation's Cybersecurity,* May 12, 2021
- Securities and Exchange Commission 17 CFR Parts 229 and 249 [Release Nos. 33-10459; 34-82746] *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*

Other U.S. Government Reports

This document is also informed by 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]

Standards, Guidelines, and Best Practices

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

- The Federal Risk and Authorization Management Program (FedRAMP), *Securing Cloud Services For The Federal Government* [https://www.fedramp.gov/]
- 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]
- Cyber Risk Institute, *Financial Services Cybersecurity Framework Profile Version 1.1* [FSP]