The attached DRAFT document (provided here for HISTORICAL purposes) has been superseded by the following publication:

Publication Number: **NIST Interagency Report 7622**

Title: **Notional Supply Chain Risk Management Practices for Federal Information Systems**

Publication Date: **10/16/2012**

- Final Publication: http://dx.doi.org/10.6028/NIST.IR.7622
- Related Information on CSRC: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7622
- Information on other NIST Computer Security Division publications and programs can be found at: http://csrc.nist.gov/

Draft NISTIR 7622

Piloting Supply Chain Risk Management Practices for Federal Information Systems

Marianne Swanson
Nadya Bartol
Rama Moorthy

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

Draft NISTIR 7622

Piloting Supply Chain Risk Management for Federal Information Systems

Marianne Swanson
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

Nadya Bartol
Booz Allen Hamilton

Rama Moorthy
Hatha Systems

June 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

Acknowledgments

The authors, Marianne Swanson, National Institute of Standards and Technology, Rama Moorthy, Hatha Systems, and Nadya Bartol, Booz Allen and Hamilton, would like to thank Mike Hawk, Department of State for his consistent and continuous contributions throughout the life of this project. We would like to acknowledge Michael Ferraiolo, National Institute of Standards and Technology, for his assistance in developing the appendices and the following authors of the *Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 Supply Chain Risk Management Pilot Program* who were instrumental in developing the initial content of this NISTIR (contributors are listed alphabetically):

Nadya Bartol
Forrest Frank
Mike Hawk
Kenneth "Crash" Konwin
Rama Moorthy
Jean Petty
Joseph Scott
David A. Wheeler (Lead)
Christine Youngblut

We would also like to thank Kurt Seidling, Department of Homeland Security, and the members of the Comprehensive National Cybersecurity Initiative 11 Lifecycle Processes and Standards Working Group and their support contractors as well as members of the Information Technology Sector and Communications Sector Coordinating Councils for their review and comments on this document. Their comments and direction were instrumental in the development of this document.

Note to Reviewers

This Draft NIST IR is intended to provide a wide array of practices that when implemented will help mitigate supply chain risk. Many of the practices are based on good security practices and procedures found in NIST Special Publications like NIST SP 800-53, *Recommended Security Controls for Federal Information System;* the National Defense University, *Software Assurance in Acquisition: Mitigating Risks to the Enterprise;* and the National Defense Industry Association (NDIA), *Engineering for System Assurance,* and then expanded upon to include supply chain-specific implications. When reviewing this document, please consider applying a few of the practices to upcoming procurements, then providing us with comments on the practicality, feasibility, cost, challenges, and successes. The Comprehensive National Cybersecurity Initiative (CNCI) Initiative 11, Develop Multi-Pronged Approach for Global Supply Chain Risk Management, is currently piloting many of the practices, though to get a much more thorough sample, it would be beneficial to have our readers "pilot" a few of the practices.

Comments on the document should be sent to: scrm-nist@nist.gov by August 15, 2010. Comments and lessons learned on piloting the practices should be sent to the same e-mail address by December 30, 2010.

Table of Contents

1. Introduction

Information systems[1] are essential for government operations. These systems and their components are at increasing risk of supply chain[2] attacks from adversaries enabled by growing technological sophistication and facilitated by the rapid globalization of our information system infrastructure, suppliers, and adversaries.

The ever broadening reliance upon globally sourced information system equipment exposes federal information systems and networks to an enlarging risk of exploitation through counterfeit materials, malicious software, or untrustworthy products.[3] Many of our suppliers are transnational. Accelerating trends in multi national mergers and acquisitions[4] of information system suppliers and integrators is making it almost impossible to adopt corporate ownership and control alone as the basis for assuring supply chain security. This is in part because these accelerating trends reduce transparency and traceability of the supply chain. Globalization and its consequences are permanent and are likely to have a greater impact over time. Even in domestically developed information system elements, intentional and unintentional weaknesses/vulnerabilities may present opportunities for supply chain-related compromises.

Supply chain attacks may involve manipulating computing system hardware, software, or services at any point during the life cycle. Supply chain attacks are typically conducted or facilitated by individuals or organizations that have access through commercial ties, leading to stolen critical data and technology, corruption of the system/infrastructure, and/or disabling of mission-critical operations.

Organizations must assess and manage supply chain risks to ensure mission success. The goal of this document is to help manage these supply chain risks by providing organizations with a defense-in-breadth toolset of supply chain assurance programmatic activities that the organization implements as well as general and technical requirements that the organization can place in contractual documents. This document represents a component of a broader supply chain risk management strategy that includes a variety of policies, standards, regulatory changes, and implementation frameworks.

1.1 Purpose

This document provides a set of practices that can be referenced or used for those information systems categorized at the FIPS (Federal Information Processing

[1] An information system is a discrete set of *information resources* organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial/process controls systems, telephone switching/private branch exchange (PBX) systems, and environmental control systems.
[2] The term “supply chain” is used in this document to mean a set of organizations, people, activities, information, and resources for creating and moving a product or service (including sub-elements) from suppliers through to an organization’s customers.
[3] For the purposes of this document, products and product components are referred to as “elements.”
[4] This document uses the terms “acquisition” and “procurement” interchangeably.

Standards) 199 high-impact level.[5] These practices are intended to promote the acquisition, development, and operation of information systems or system-of-systems[6] to meet cost, schedule, and performance requirements in today's environment with globalized suppliers and active adversaries. Integrated within the information systems development life cycle (SDLC), these practices provide risk mitigating strategies for the acquiring federal agency to implement.

In order to ensure that the practices get included in the procurement process and contractual documents, organizations must first establish a methodology for handling supply chain risk. This document walks the reader through:

- Determining which procurements should consider supply chain risk;
- Working with the procurement office, legal counsel, information system security personnel, and other appropriate agency stakeholders to help mitigate supply chain risk through the careful selection of security and supply chain contractual requirements;
- Resolving residual supply chain risk by requiring either the contractor or the organization to implement additional applicable practices contained in this document and augmenting the baseline of security controls[7] defined for the information system; and
- Describing the roles and responsibilities within the organization as they relate to supply chain risk management.

This document does not provide specific contract language, threat assessment, or a complete list of supply chain assurance methods and techniques that mitigate specific supply chain threats; instead, it emphasizes a short list of practices and provides basic information about them. It is our intent that organizations begin to pilot the activities and the practices contained in this document and provide feedback on the practicality, feasibility, cost, challenges, and successes. This is the first step in a much larger initiative of developing a comprehensive approach to managing supply chain risks. NIST intends to expand this document into a NIST Special Publication after many of the practices and organizational structure and methodologies have been piloted under the auspice of the Comprehensive National Cybersecurity Initiative (CNCI) Initiative 11, Develop Multi-Pronged Approach for Global Supply Chain Risk Management. Section 1.3 provides additional information about the initiative.

[5] To comply with the federal standard, organizations must first determine the security category of their information system in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* then derive the information system impact level from the security category in accordance with FIPS 200.

[6] In certain situations within an organization, an information system can be viewed from both a logical and physical perspective as a complex *system-of-systems* (e.g., Federal Aviation Administration National Air Space System) when there are multiple information systems involved with a high degree of connectivity and interaction among the systems.

[7] NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government.

1.2 Scope

This document is an important part of the CNCI Initiative 11; however it is only a small part. It is important to note that in conjunction with this document there are plans for legislative changes, Federal Acquisition Regulation (FAR) modifications, policy and internal policy, employee and contractor training, commercial and government standards, and new supply chain risk management frameworks, processes, capabilities and tools. The CNCI Initiative 11 understands that the security of the supply chain for federal information systems is a relatively new problem and solutions, methods, techniques, approaches and tools are expected to evolve. Over time a repeatable process is expected to emerge to use data collected by acquirers, integrators and suppliers to improve organization supply chain risk management practices and start to correlate the benefits acquirers may gain in return for the higher costs imposed on them and industry resulting from the implementation of these practices. It is expected that the implementation of practices described in this document, as well as the implementation of other future pieces of the supply chain risk management strategy will require resources to implement throughout the acquirer, integrator, and supplier community. The resources will be based on the future implementation details and as such are outside the scope of this document.

The supply chain encompasses the full product life cycle and includes design, development, and acquisition of custom or commercial off-the-shelf (COTS) products, system integration, system operation (in its environment), and disposal. People, processes, services, products, and the elements that make up the products wholly impact the supply chain. This document focuses on countering supply chain risks throughout the life cycle, not just on accepting system products/elements “as they are” and managing their risks after delivery. An individual practice may only partly reduce supply chain risks, because there are many actors and elements in real system supply chains. Therefore, this document uses a combination of practices, applied throughout the SDLC, to optimally decrease supply chain risks. Organizations should select these practices based on their suitability for a specific application or acquisition and combined impact on the system’s performance, cost, and schedule.

This document is intended to serve a diverse audience including information system owners, acquisition staff, information system security personnel, and system engineers responsible for delivering information systems with supply chain assurance. This includes those in government and in commercial companies producing information technology products (or COTS or government off-the-shelf [GOTS] elements as is expressed throughout the document), services, and systems as well as providing information security services.

A supplier of information technology elements or services is also an acquirer of sub-elements that make up the products. Each organization that performs the role of an acquirer should perform supply chain risk management activities and flow down those supply chain requirements to its sub-tiers (e.g., through requests for proposals and contracts). Acquirers should ensure through appropriate contract language that if any proprietary data is obtained, the contract specifies how the data will be used, how long it will be kept, who it can be shared with or what intellectual property protections will prevail. Supply chain issues should be considered when developing request for

information (RFI), solicitations of all types (e.g., requests for quotation [RFQ], requests for proposal [RFP]), Cooperative Research and Development Agreements (CRADAs), grants, and similar documents. Articulate measurable and enforceable requirements in all agreements and procurement documents. To the maximum extent practicable, use existing standards and guidelines to increase assurance that the processes are performed.

Information system owners must take the lead in coordinating and implementing supply chain activities for their information systems. Supply chain risk is measured by the likelihood and severity of damage if the information system is compromised, which includes an assessment of the importance of the system and the impact of compromise on organizational operations and assets, individuals, other organizations, and the Nation. Organizations should consider the security categorization of the information system when applying the supply chain practices. Not every information system should implement supply chain risk mitigation strategies. The FIPS 199 impact level should aid the organization in determining the appropriate level of assurance.

1.3 Background

The President's Comprehensive National Cybersecurity Initiative (CNCI) Initiative 11 is co chaired by the Department of Defense (DoD) and the Department of Homeland Security (DHS). The initiative will provide federal agencies with a standard, well-understood toolkit of technical and intelligence resources to manage supply chain risk to a level commensurate with the criticality of information systems or networks. This integrated approach is based on the work of subject matter experts operating across the government.

Under the CNCI Initiative 11, a DoD Supply Chain Risk Management (SCRM) Pilot Working Group was assembled to prepare materials for several supply chain pilots within DoD. The pilots will "exercise system-and network-level mitigations of supply chain risk to inform guidance, resourcing, and the planning for training of supply chain professionals."[8]

The SCRM Pilot Working Group evaluated a large set of existing material and developed a set of key practices for supply chain risk management. The working group examined a number of sources including the National Defense Industrial Association's (NDIA) *Engineering for System Assurance*; National Defense University, *Software Assurance in Acquisition: Mitigating Risks to the Enterprise;* Department of Homeland Security's (DHS) *Build Security In* Web site;[9] National Institute of Standards and Technology (NIST) Special Publications : SAFECode's *Fundamental Practices for Secure Software Development*; industry standards; the Committee on National Security Systems Global Information Technology Working Group's (GITWG) *Framework for Lifecycle Risk Mitigation for National Security Systems in the Era of Globalization*; emerging practices of selected federal agency programs; and information from subject matter experts. The review of these documents led to the development of a set of supply chain assurance methods/techniques or practices that

[8] SCRM Implementation Plan_17Jan08 v.2
[9] https://buildsecurityin.us-cert.gov/daisy/bsi/home.html

cover the full SDLC as part of a government wide supply chain risk management solution. Using these practices as a foundation, the Civilian Key Practices Working Group[10] developed this document in support of implementing civilian agency supply chain pilots as well as providing a set of practices organizations can implement now to reduce their supply chain risk. A practice was selected from this material if the practice met all of the following criteria:

1. The practice is known and can be applied now (no research is required for initial use);
2. Implementing the practice will have a significant positive impact in countering supply chain risks; and
3. The estimated cost and schedule impact of the practice is reasonable (for at least some circumstances).

1.4 Life Cycle Standards

The supply chain initiative is striving to address supply chain risks government wide, though the government's information system supply chain includes a large commercial base. Organizations use many different system development life cycle representations, systems engineering process frameworks, and enterprise architecture frameworks. This document uses the life cycle phases contained in NIST Special Publication 800-64, Rev. 2, *Security Considerations in the System Development Life Cycle.*

1.5 Prerequisites for Successful Supply Chain Risk Management (SCRM) Implementation

When information systems services and COTS/GOTS elements are being considered, it is essential that the acquiring organization employ or require standard, good design and development principles and practices. The implementation of effective supply chain risk management begins with the fundamental performance of good system design and development practices. Examples of good practices are:

- Integrate information system security requirements from inception – do not wait until late in the life cycle.
- Ensure your information system security, acquisition personnel, legal counsel, and other appropriate advisors and stakeholders are participating in decision making from system concept definition/review and are involved or approving each milestone decision.
- Ensure you have funding allocated for information system security and supply chain risk management – without funding, nothing will happen.
- Follow consistent, well-documented, repeatable processes for system engineering and acquisition. Adjust documentation as changes dictate.
- Develop, implement, and test a contingency plan to include the supply chain to ensure integrity and reliability of supply even during adverse events (e.g., natural disasters such as hurricanes or economic disruptions such as labor

[10] The Civilian Key Practices Working Group consists of members from NIST, DHS, and the Department of State. This group is a sub group of the Supply Chain Risk Management Working Group #2: Lifecycle Standards and Processes.

strikes). Such plans may incorporate the use of multiple suppliers or multiple supply chains.

- Proper oversight of suppliers. This includes actively managing suppliers through contracts/Service-Level Agreements (SLAs).
- Audit the development process. Use trusted third-party auditing mechanisms in the life cycle for assessing the exit criteria for each life cycle step (e.g., vetting the requirements analysis, architecture design).
- Perform quality assurance and quality control, e.g., of security features.
- Assign roles and responsibilities, so that involved individuals know who is responsible and has the required authority to take action, who is accountable for an action or result, who must be consulted, and who must be informed.
- Fully implement the appropriate tailored set of baseline security controls in NIST SP 800-53 required by the FIPS 199 impact level.

2. Implementing Supply Chain Risk Management

In order to effectively mitigate supply chain risk, organizations need an integrated approach to assess and mitigate supply chain risk. The development of organization-wide policy and procedures that outline the roles and responsibilities of all stakeholders is the first step in implementing a supply chain risk management program. Organizations should develop procedures for determining which information systems will implement supply chain mitigation strategies based on the SDLC phase, the FIPS 199 security categorization, and the FIPS 200/NIST SP 800-53 impact level of the information system. Note that NIST SP 800-53 specifies supply chain protection for information systems at the high-impact level.

This chapter provides an approach to establishing a Supply Chain Risk Management Capability (SCRMC) within an organization to enable information system owners, information security professionals, and procurement officials to make informed decisions on the assurance of the supply chain when procuring services and procuring and operating hardware or software.

2.1 Supply Chain Risk Management Capability (SCRMC)

Implementation of a SCRMC will require an agency to establish a coordinated team approach to assess the supply chain risk and counter the risks by using technical and programmatic mitigation techniques. The composition of the team, either ad hoc or formal, will enable the members to conduct a comprehensive analysis of the supply chain, communicate with external partners/stakeholders, and assist them in developing a supply chain strategy for any given acquisition.

Organizations should develop a supply chain risk management policy that establishes the organizational structure that defines roles and responsibilities for implementing supply chain risk mitigation activities. Operational procedures for the SCRMC should be written and approved. The procedures should describe who conducts assessments, performs analysis, makes risk decisions, and prepares the procurement-related documents, and specifies any specific training requirements. Figure 1 represents a team approach that illustrates the organizational structure of a supply chain risk management capability.

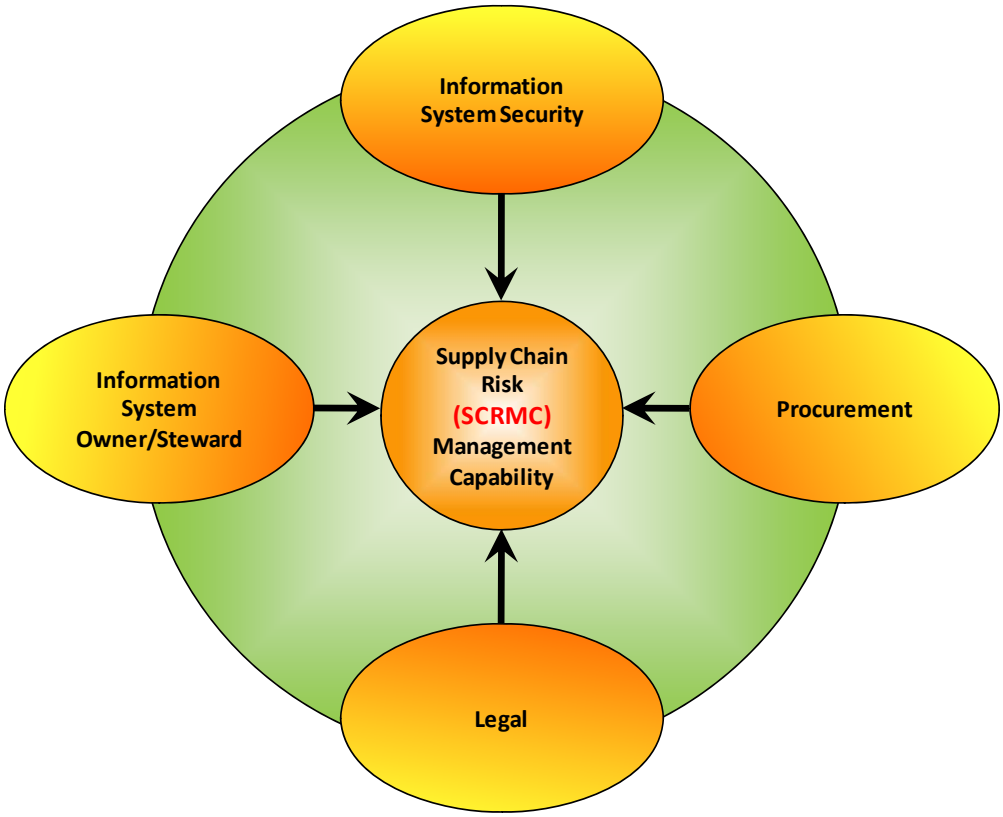

Figure 1 – SCRM Capability

2.2 Roles and Responsibilities

The SCRMC should consist of personnel that can assess the likelihood and method of attack, and bring the expertise required to identify and recommend a regimen of technical mitigations. The strategies and mitigations must comply with the Federal Acquisition Regulation (FAR) as well as other organizational policies and procedures. Managing the supply chain is an organization-wide activity with several roles and responsibilities beyond the SCRMC. Note that the names and roles will vary among organizations. In some organizations, a single individual may hold multiple roles.

Authorizing Official (AO) - An AO is a senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of supply chain risk to organization operations and assets, individuals, other organizations, and the Nation.

Chief Information Officer (CIO) - The CIO is responsible for the organization's information system planning, budgeting, investment, performance, and acquisition. As such, the CIO provides advice and assistance to senior organization personnel in acquiring the most efficient and effective information system to minimize supply chain risks within the organization's enterprise architecture.

Contracting Officer - The Contracting Officer is the person who has the authority to enter into, administer, and/or terminate contracts and make related determinations and

findings. The Contracting Officer will use their expertise to develop an acquisition strategy that alone, or with technical mitigations, will reduce supply chain risk.

Contracting Officer's Technical Representative (COTR) - The COTR is a qualified employee appointed by the Contracting Officer to act as their technical representative in managing the technical aspects of a contract.

Legal Advisor/Contract Attorney - The legal advisor is responsible for advising the team on legal issues related to the acquisition process.

The Risk Executive (Function) - is an individual or group within an organization that helps to ensure that SCRM-related considerations for individual information systems are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization. In carrying out its core missions and business functions SCRM associated with individual information systems and ensures procurements are consistent across the organization. Procurements should reflect organizational risk tolerance, and is considered along with other types of risks in order to ensure mission/business success.[11]

Information Owner/Steward - The information owner/steward represents the business and programmatic interests in the information system during the SDLC process. The information owner/steward plays an essential role in supply chain security by being aware of functional system requirements. The information owner/steward along with information security professionals must determine if the supply chain practices selected are sufficient to mitigate supply chain risks.

Information System Owner - The information system owner is responsible for the procurement, development, integration, modification, operation, and maintenance of an information system. The information system owner works closely with the AO, SAISO, ISSO, and the Contracting Officer to ensure that supply chain risk mitigation strategies are selected, implemented and operating as intended.

Senior Agency Information Security Officer (SAISO)/Chief Information Security Officer (CISO) - The SAISO, also known as Chief Information Security Officer, is responsible for promulgating policies on security integration in the SDLC and the development and implementation of security policy, guidelines, and procedures pertaining to supply chain risk management. The SAISO plays a leading role in introducing an appropriate structured methodology to help identify, evaluate, and minimize supply chain risks to the organization. In addition, the SAISO is responsible for analyzing and developing:

- Procedures for performing, analyzing, and utilizing integrator/supplier assessments; and
- Technical mitigation strategies derived from the integrator/supplier assessments.

[11] Adopted from NIST SP 800-37, Guide for Applying Risk Management Framework to Federal Information Systems.

Information System Security Officer (ISSO) – The Information System Security Officer is responsible for mitigating supply chain risk throughout the information system life cycle. The ISSO assesses the supply chain risk as it applies to the sensitivity of the information/data stored or processed on the information system.

Information Technology Investment Board (or equivalent) - The Information Technology (IT) Investment Board, or its equivalent, is responsible for managing the Capital Planning and Investment Control (CPIC) process defined by the Clinger-Cohen Act of 1996 (Section 5). The IT Investment Board should be aware of supply chain risks and the need to reduce the risk on selected procurements.

2.3 Supply Chain Risk Management Capability (SCRMC) Implementation

Information system owners should collaborate with SCRMC to ensure proper SCRM for the systems, elements, and corresponding SCRM services. This section describes the activities that take place to mitigate supply chain risk during the life cycle of the project using the foundation of FIPS 199, NIST SP 800-53, and good system life cycle processes and practices.

Supply chain risks should be identified by the information system owner, information system security personnel, stakeholder representatives, and possibly, outside experts to provide unbiased input. There are several methods of compiling potential risks including reviews of current and historical project documentation, brainstorming, interviewing of stakeholders, checklists, marketing analysis of potential suppliers, and Standard Operating Procedure (SOP) review.

Once the risks have been identified, information system owners should consult and coordinate with advisors, and decision makers, including technical leads, the contracting officer, and legal counsel to identify a set of SCRM-related requirements for the program including trading supply chain and related risks with other program issues (i.e., cost, performance, and schedule). Chapter 3 can be used as a source of a detailed set of activities that the organization can implement and corresponding general and technical requirements for suppliers and integrators.

The security control baseline provided in NIST SP 800-53 is the foundation or starting point for determining the needed set of security controls for an information system. In many cases, specific security controls or control enhancements will be needed to address specific threats to and vulnerabilities in, an information system. If an organization deems that certain information systems categorized at the FIPS 199 moderate-or high-impact level need to address specific threats, then an integrated SCRM procurement process is needed to analyze potential supply chain risks and implement additional security controls and/or SCRM practices as needed. Figure 2 represents the integrated SCRM Procurement Process.

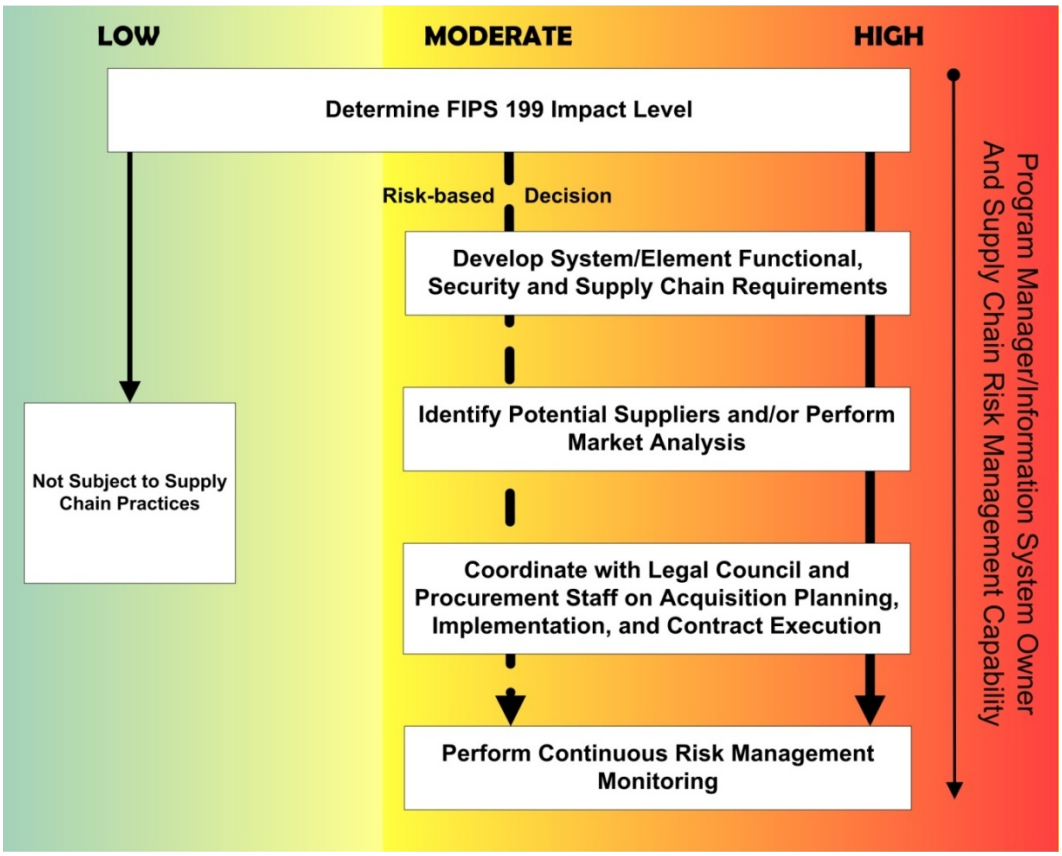

Figure 2 – Integrated SCRM Procurement Process

2.3.1 Determine Federal Information Processing Standards (FIPS) 199 Impact Level

Not every information system acquisition is a candidate for assessing supply chain risk or incorporating supply chain mitigation language into procurement documents. NIST SP 800-53, Rev. 3, Appendix F, Security Control Catalog, requires for those information systems categorized at the FIPS 199 high-impact level to implement the security control SA-12 Supply Chain Protection:

> ***SA-12***
> ***Control:*** The organization protects against supply chain threats by employing: [*Assignment: organization-defined list of measures to protect against supply chain threats*] as part of a comprehensive, defense-in-breadth information security strategy.
>
> ***Supplemental Guidance:*** A defense-in-breadth approach helps to protect information systems (including the information technology elements that compose those systems) throughout the system development life cycle (i.e., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). This is accomplished by the identification, management, and elimination of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to mitigate risk.

For information systems categorized at the FIPS 199 moderate- or low-impact level, implementation of SA-12 is not required. In the case of systems at the moderate-

impact level, it is up to the authorizing official to make a risk-based determination whether SA-12 or its components are needed.

2.3.2 Develop Requirements

The information system owner should develop a Statement of Work (SOW) that includes a detailed description of the specific technical security requirements and qualifications to include the selected SCRM practices (general and technical requirements and validation and verification activities) and NIST SP 800-53 controls relevant to an integrator and supplier and in some instances a supplier performing acquirer activities. The SOW must be a very clear and concise document and include the performance measures, evaluation criteria, and thresholds against which the respondents will be measured.

a) Determine the appropriate level of risk distribution among the acquirer, integrator, and supplier. State integrator's and supplier's level of responsibility for supplying trustworthy systems and elements in contracts.
b) Use past performance of the integrator/supplier for indications of security consciousness in their processes and the resulting systems, elements, and services as a gauge for their supply chain assurance practices. Indicators include available information about systems, elements, and services with security that is on by default, evidence of attempts by the supplier to reduce vulnerabilities, and what past vulnerabilities indicate about product/service strength, speed of patching, supplier pattern of addressing identified vulnerabilities, and current known yet unfixed vulnerabilities. Note that suppliers may weigh need to know for existing but unfixed vulnerabilities against risk of exploitation. Since past performance is no guarantee of future result, examine to see if there is a recent major change in the integrator/supplier organization that might invalidate past performance.
c) Establish requirements for processes (including test and evaluation processes) and include them in contract documents.
d) Examine how integrators select/manage their suppliers and whether or not the integrator/supplier imposes similar requirements on their suppliers.
e) Require respondents to provide a Supply Chain Risk Management Plan that addresses, in detail, their internal and external practices and controls employed to minimize the risk posed by counterfeits, and known and unknown vulnerabilities in systems, elements, and services.

2.3.3 Identify Potential Suppliers and/or Perform Market Analysis

Once the information system owner defines the requirements, potential integrators/suppliers may be needed. Potential integrators/suppliers can be identified by several methods; 1) sending out a "*sources sought*" document; 2) sending out a request for information document (RFI); or 3) performing a market survey to obtain prices from potential suppliers.

Information system owners should identify known and potential sources of supply (including qualified integrators/supplier and qualified product lists). If the information system owner does not know who the potential integrators/suppliers are or would like to discover alternative integrators/suppliers or the suppliers of the integrators/suppliers (the chain in depth), the information system owner working with the contracting officer should conduct a market analysis. The market analysis should identify which companies can provide the required items or make suggestions of possible options. The various identification methods should determine if all items under the requirement can be obtained from one integrator/supplier or a number of them. Potential integrator/supplier information can also be gathered from open sources, such as the press, Internet, periodicals, and fee-based services. Information system owners should be aware that respondents may include integrators/suppliers not previously identified.

Listed below are some of the sources that are available including a brief description of the type of information provided:

Central Contractor Registry (CCR) – CCR is the primary registrant database for integrators and suppliers conducting business with the U.S. federal government. CCR collects, validates, stores, and disseminates data in support of agency acquisition missions.

Commercial and Government Entity (CAGE) Code – A CAGE Code identifies companies doing or wishing to do business with the federal government. The code is used to support a variety of mechanized systems throughout the government. The code provides for a standardized method of identifying a given facility at a specific location. The code may be used for a Facility Clearance, a Pre-Award survey, automated Bidders Lists, pay processes, source of supply, etc. In some cases, prime contractors may require their sub contractors to have a CAGE Code.

Dun and Bradstreet (DUNS) - Dun and Bradstreet is a provider of business information from public records (includes suits, liens, judgments and bankruptcies, and other government information). They also provide entity matching to determine the structure of a business' affiliations.

Business Identification Number Cross-Reference System (BINCS) - BINCS is a search engine of manufacturers and suppliers. Information in this system is cross-referenced to permit inquiry by CAGE, DUNS, company name, telephone number, Standard Industrial Classification (SIC) code, and ZIP code. Information about the supplier is returned from the CAGE File, the CCR File, and the Joint U.S./Canada Certification Program. BINCS provides linkages to each of these source systems for an expanded view of the trading partner's profile.

The information gathered during pre-solicitation may indicate a type of risk and/or likelihood that a particular risk is prevalent in a specific industry. For example, foreign manufacturing introduces the risk that foreign interests (individual, organization, or nation state) have the power, direct or indirect, to decide matters affecting the management or operations of companies within an industry in a manner that may

result in risk to the information system, organization, or Nation. These acts could include the introduction of malware into software or hardware components that would allow remote, unauthorized access to an information system resulting in denying availability, corrupting the information, or accessing the data for criminal use. The presence of foreign manufacturing alone is no reason to employ special supply chain risk mitigation practices, as the supplier must be evaluated in its entirety.

2.3.4 Coordinate Acquisition Activities

Working with the members of the SCRMC, the procurement official, with the assistance from the information system owner, information security personnel, and legal counsel, should develop the procurement strategy (Acquisition Plan) that best supports the selected project/program and includes:

- A list of potential sources of supplies/services that could meet the need, the extent and results of the market research and their impact on the various elements of the plan;
- A description of how competition will be sought, promoted, and sustained throughout the course of the acquisition process;
- A description of various contracting considerations, including contract type and the use of performance-based contracts (See Part 16 of the FAR for a description of different contract types.);
- Information security and supply chain risk mitigation strategies and practices based upon the (known) potential sources of suppliers/service providers that could meet the program requirements and the impact suppliers may have on various elements of the element/system; and
- Identification and application of relevant acquisition policies and contract clauses to ensure that authorities necessary and sufficient to verify the element, the element processes, the business processes of the supplier acquirer and supplier.

Additionally, any legal issues should be disclosed, the type of contract(s) that will be in the government's best interest should be identified, and a decision made whether one or more integrators/suppliers will be required in order to meet program needs. See Part 7.105 of the FAR for a complete list of acquisition plan of action subcomponents.

Once the integrator/supplier responds to the statement of work and presents a proposal, the information system owner, as part of a Technical Evaluation Panel (TEP), will perform a technical review, and the Contracting Officer will conduct the cost review to determine which proposal is the most beneficial (best value) to the government.

The TEP (or similar entity) will measure the quality of each integrator/supplier response against pre determined, weighted evaluation factors to gauge the quality of each proposal. The TEP should look for documented evidence of a integrator's/supplier's claim to meet the desired security/SCRM requirements, such as the supplier's demonstrated record, as confirmed by references, of successful past performance of the same or substantially similar contract efforts, including quality of

services or supplies, timeliness of performance, cost control, and the integrator's/supplier's business relations.

2.3.5 Perform Continuous Monitoring

Once a system becomes operational, the suppliers, elements, delivery processes, and business processes (among others) may change. These changes may alter or add supply chain risks. During operations, continue to perform supply chain risk management. An established relationship with an integrator/supplier that understands supply chain risk and provides information on any changes to the element, environment, vulnerabilities, and patches on an ongoing basis helps to manage supply chain risk. The following are a set of activities that will help to maintain supply chain oversight:

- Record SCRM lessons learned and disseminate them for future use, both within the project and within the larger organization(s).
- Monitor and periodically (or continuously if appropriate) reevaluate changes in risk, suppliers, operational environment, and usage. Then respond where appropriate. Note: (1) Use information as available, including information from commercial sources, U.S. government agencies, and intelligence information as appropriate. (2) Respond to such changes when appropriate, e.g., by adding additional countermeasures (such as additional practices from this document) or changing to a less-risky supplier.

Supply chain risks should be considered when acquiring replacement components or field additions/modifications/upgrades, particularly if they do not go through traditional acquisition processes that examine supply chain risks. Obsolescence of subsystems is a risk driver because they are intended for use over an extended time, leaving them vulnerable to obsolescence of the parts, subsystems, and technologies that compose the system. Systems that have a long standard life cycle may require a substantial number of components that are no longer available from the original component manufacturer or through their franchised distributors. An obsolescence program might be required when components become unavailable through authorized supply channels, to engage procurement activities from the open market. Because of the nature of the open market channel, the risk of encountering substandard, subverted, and counterfeit products may increase.

- When purchasing (including rapid acquisition), where possible, purchase only elements/services known to have been previously screened for supply chain risks (including counterfeits and subversion).
- Consider advance purchase and inventory of spare parts while they are widely available and verifiable and can be installed by trained and knowledgeable authorized service personnel.
- Consider supply chain risks when acquiring replacement components or field additions/modifications/upgrades, particularly if they do not go through traditional acquisition processes that examine supply chain risks.

3. Supply Chain Risk Management Practices

When organizations are determining their information technology needs for new or modified mission/business programs, organizations should consider the FIPS 199 impact level of the information that the information system will process. If the data is determined to be a FIPS 199 high-impact level, then in accordance with NIST SP 800-53, security control SA-12, the organization protects against supply chain threats by employing an organization-defined list of measures as part of a comprehensive, defense in-breadth information security strategy.[12] This chapter provides twenty-one practices that an organization should consider when creating the list of measures that they will employ as part of their information security strategy.

Each practice is a blend of programmatic activities, validation/verification activities and requirements, as well as general and technical requirements. The programmatic and validation/verification activities are implemented by the acquiring organization. The term "Acquirer" is used throughout the practices to mean the federal agency acquiring the product or element. The term "element" is used throughout to mean a commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) software, hardware and firmware and is synonymous with components, devices, products, systems, and materials. An element is part of an information system and may be implemented by products or services. Table 1 describes how the practices are formatted by role, activities, and requirements.

In many cases, the practice will apply to a software supplier and a hardware supplier. Since most hardware devices contain some level of firmware or software, the document does not differentiate between types of suppliers. The term "integrator" is used to depict a third-party organization that specializes in combining products/elements of several suppliers to produce elements (information systems). The term "supplier" is used to depict an organization that produces elements and provides them to the integrator to be integrated into the overall system; it is synonymous with vendor and manufacturer. Supplier in this document also applies to maintenance/disposal service providers. Appendix A provides a glossary of terms used throughout the document.

A description is provided at the beginning of each practice that depicts the intent of the practice. The practice then expands into specific activities and requirements that will aid in obtaining varying levels of supply chain assurance. In some cases, the practice or a portion of the practice may be too costly, not applicable or feasible to implement for a FIPS 199 high-impact information system. The practices are recommendations and should be considered based on a risk management approach. The practices selected for this document take into account that the organization has a developed and implemented robust information security program and uses NIST guidelines and standards.

[12] SA-12 provides seven control enhancements that may be applied by an organization to increase the level of supply chain assurance. The seven enhancements are included within Chapter 2 and the following practices: 3.1, Maximize Acquirer's Visibility into Integrators and Suppliers; 3.15, Harden Supply Chain Delivery Mechanisms; 3.5, Enable Diversity; and 3.11,Testing.

The twenty-one, practices if implemented in their entirety, cover the complete system development life cycle, beginning with the first practice, 3.1, Maximizing Acquirer's Visibility, which suggests that the acquirer should seek to maximize visibility into all integrators and suppliers and their supporting tiers to the final practice, 3.21, Reduce Supply Chain Risks During Disposal, which addresses the need for secure disposal to ensure the element or data does not harm, lose, or corrupt the acquirer's sensitive information.

There are a number of potential supply chain risk management practices that can be applied to an information system or elements of an information system. In a particular information system, different practices may be applied to varying elements (e.g., one set for the supplier providing a COTS portion of the information system and another for the integrator developing a custom application). Table 1 reflects the types of actions and their descriptions an Acquirer, Integrator, and Supplier would implement for each SCRM practice selected. The information system owner along with information security professionals must determine if the practices selected are sufficient to mitigate supply chain risks. The information system authorizing official will make the final decision as to the acceptable level of risk.

Acquirers should appropriately protect integrators' and suppliers' data, and integrators should appropriately protect supplier's data that will be collected as a result of implementing specific practices provided in this document. The details of this protection should be appropriately documented in contractual language that specifies how the data will be used, how long it will be kept, who it can be shared with or what intellectual property protections will apply.

Table 1 – Practice Format

Role	Type of Action	Description of Action
Acquirer	Programmatic Activities	Practices that an acquirer will undertake within their programs, including requirements to be included in contractual documents, as well as internal policies and procedures.
Integrator	General Requirements	General practices that an integrator will implement within their programs that are either in response to contractual requirements or to demonstrate existence of programmatic activities that reduce supply chain risk.
Supplier	General Requirements	General practices that a supplier will implement within their programs that are either in response to contractual requirements or to demonstrate existence of programmatic activities that reduce supply chain risk.
Integrator	Technical Implementation Requirements	Detailed technical practices that an integrator will implement within their programs to demonstrate technical capabilities to manage supply chain risk.

Supplier	Technical Implementation Requirements	Detailed technical practices that a supplier will implement within their programs to demonstrate technical capabilities to manage supply chain risk.
Integrator	Validation and Verification Requirements	Suggestions on how an integrator can demonstrate that they have implemented SCRM.
Supplier	Validation and Verification Requirements	Suggestions on how a supplier can demonstrate that they have implemented SCRM.
Acquirer	Validation and Verification Activities	Suggestions for how an acquirer can ascertain that integrators or suppliers have implemented SCRM.

3.1: Maximize Acquirer's Visibility into Integrators and Suppliers

Acquirers should seek to maximize visibility into all integrators and suppliers and their supporting tiers (including custom, COTS/GOTS and open source products). The purpose of this is to understand how elements are selected, created, tested, delivered, supported and protected throughout the element life cycle. Acquirers should use this knowledge of the integrators and suppliers supply chain practices to assess trade-offs between the acquirers risk tolerance, performance requirements, and resource constraints.

3.1.1 Acquirer - Programmatic Activities

a) Develop source selection criteria and procedures that encourage integrators and suppliers to provide detailed visibility into elements, services, and processes as part of their submissions for contracts.
b) Develop approaches that encourage integrators and suppliers to gain visibility and transparency into their supply chains as deeply as possible and reasonable. (1) Develop incentives that reward integrators and suppliers for providing program-specific detailed technical information and technical data on products and services throughout their life cycle; and (2) include requirements that address the selection of open source elements.
c) Encourage and provide incentives for integrators and suppliers to deliver, for the life span of the contract, up-to-date information on changes that affect Supply Chain, SC, risk to the system and elements throughout their life cycle, such as changes in their suppliers, locations, process, and technology.
d) Develop and document, for open source elements, requirements for acceptance criteria and procedures.
e) Prefer integrators who will provide technical details about their system/service, including designs (such as blueprints, schematics, architectures, and interfaces). Such information may also be important to enable later support should the integrator stop supplying the system/service.

f) Prefer integrators who understand, evaluate, and document elements (including open source) and element processes that could result in weaknesses or vulnerabilities and if exploited, could result in loss or compromise.
g) Define criteria for the types of evidence including measures, activities, behaviors, and test results in conformance with specifications and standards, compliance with statutory or regulatory requirements and with contract terms and conditions as they are applied to the production and delivery of systems/services.
h) Prefer suppliers who understand supply chain characteristics, for both physical and logical (e.g., electronic) delivery of products (including open source) and services.
i) Prefer integrators and suppliers who maintain transparency about themselves, their elements, and their suppliers. For example, select integrators and suppliers who proactively provide all known errata for their elements and services (some errata may have vulnerability implications).

3.1.2 Integrators - General Requirements

a) Prefer suppliers who maintain transparency about themselves, their elements, and their suppliers. For example, select suppliers who proactively provide all known errata for their elements and services (some errata may have vulnerability implications).

3.1.3 Suppliers - General Requirements

a) None

3.1.4 Integrators - Technical Implementation Requirements

a) Understand, evaluate, and document elements (including open source) and system processes that could result in weaknesses and vulnerabilities and if exploited, may lead to the loss or compromise of confidentiality, integrity, or availability. Examples of such documentation include: form, fit, and function of the element; packaging, assembly, manufacture, and test processes and procedures; materials used to create, package, and sustain the element; relevant knowledge, and integration processes.
b) Document resources, activities, behaviors, and test results that provide evidence of deviations and conformance to specifications and standards, compliance with statutory or regulatory requirements and contract terms and conditions for production and delivery of system and associated elements including supply chain processes.
c) Prefer suppliers who are able to provide technical details about their elements and/or services where appropriate. Examples of information may include

interfaces specifications, configuration details, element processes, and any known weaknesses and vulnerabilities. Such information may be important to enable follow-on support, including when element /service is no longer available.

3.1.5 Suppliers - Technical Implementation Requirements

a) Provide evidence of deviations and conformance to specifications and standards, compliance with statutory or regulatory requirements and contract terms and conditions for production and delivery of elements including supply chain processes. Examples include processes, activities, behaviors and test results where available. Certifications and compliance validation, such as Common Criteria, FIPS 140-2 validation, or other element certifications, are applicable here.

3.1.6 Integrators - Validation and Verification Requirements

a) Evaluate and document supply chain characteristics, for both physical and logical (e.g., electronic) delivery of system, processes and elements.
b) Review activities, behaviors, and test results that provide evidence of implementation of security practices within the integrators supply chain against contractual requirements.
c) Use acceptance testing processes and methods on COTS or GOTS or other elements (including open source).
d) For subcontractors, use acceptance testing processes and methods on COTS or GOTS or other elements (including open source).
e) Detect and assess weaknesses and vulnerabilities that would result in compromise of elements, supply chain processes, or personnel in the supply chain.
f) Validate supplier-documented technical and security activities, and report findings to the project or program manager, information system owner, Contracting Officer, Contracting Officer’s Technical Representative, etc.).

3.1.7 Suppliers - Validation and Verification Requirements

a) Evaluate and document supply chain characteristics, for both physical and logical (e.g., electronic) delivery of elements.
b) Detect and assess weaknesses and vulnerabilities that would result in compromise of elements, supply chain processes, or personnel in the supply chain.

3.1.8 Acquirer - Validation and Verification Activities

a) Verify that the integrator has the ability to monitor supplier activities to detect and assess threats or attempts to gain or exploit exposure of or access to elements, supply chain processes, or supply chain actors.
b) Review and verify that integrator security policies, procedures, and activities are executed throughout the system/service life cycle. The purpose is to identify supply chain process weaknesses or vulnerabilities that, if exploited, could result in the loss or compromise of confidentiality, integrity, or availability.

3.2: Protect Confidentiality of Element Uses

The disclosure of element uses, processes, systems, or information by suppliers, integrators, or acquirers without clear understanding of the consequences of disclosure should be minimized. Use approaches that share system characteristics and user information only to the extent needed to assure successful accomplishment of acquisition objectives balanced with security risk. This information should be limited to the information necessary and sufficient to design, develop, test, produce, deliver, and support the system/element.

3.2.1 Acquirer - Programmatic Activities

a) Develop and employ acquisition and procurement policies, procedures, vehicles, and processes that establish restricted access to information by potential suppliers or integrators. The intent is to prevent such information, alone or in aggregation with other data or information available from other sources, from being combined in such a manner as to compromise the confidentiality of element uses.
b) When developing requirements, minimize exposing the uses of the system and its elements, as well as the processes by which elements are designed, developed, produced, tested, delivered, or supported.
c) Limit the following information: what the system is, the functions of the system; the other systems it will interface with; the missions the system supports; when or where the system elements will be bought/acquired; and how many system instances there will be, or where the system may be deployed. The limitations on information sharing may differ for different parties and at different times (e.g., before, during, and after acquisition). More information must typically be shared with custom developers; in such cases, use other practices to reduce risk.[13]
d) Based on the risk requirements of the mission and organization, consider using a centralized intermediary to acquire elements.
e) Centralize support and maintenance services to minimize direct interactions which may expose confidentiality of system uses.

[13] Examples of other practices to reduce risk are Defensive Design, Formalized Service and Maintenance, Testing, Protect Supply Chain Environment, and Promote Awareness, and Educate, and Train Personnel on Supply Chain Risks.

f) Diversify/disperse how the product is acquired in order to make it difficult for an adversary to determine how, when, and where an element will be acquired. When appropriate to make the supply route less predictable, consider dynamic sourcing [14] from trusted suppliers.
g) Prefer integrators and suppliers who can support centralized and/or dispersed buying approaches upon request.

Note: Acquirers should note that when information is withheld from the supplier or integrator, it may be more difficult for them to help the acquirer select the right element or product for its intended use, or to use the element or product appropriately. Additionally, when information is withheld from the supplier or integrator, opportunities for innovation might be missed. Acquirers are responsible for understanding and articulating their needs and considering the risks and the benefits associated with releasing or withholding information from their suppliers or integrators.

3.2.2 Integrator - General Requirements

a) Protect against disclosing uses of system, elements, or processes by which elements are designed, developed, produced, tested, delivered, or supported, or convey technological or operational advantage.
b) Limit the following information (including any metadata): the identity of the user or developer; the functions of the system; the other systems it will interface with; the missions the system supports; when or where the system elements will be bought/acquired; how many system instances there will be, or where the system may be deployed. The limitations on information sharing may differ for different parties and at different times (e.g., before, during, and after acquisition). When more information must typically be shared with custom developers in such cases, use other practices to reduce risks.
c) Diversify/disperse how the element is acquired to make it difficult for an adversary to determine when and where an element will be acquired. If the element can appropriately be sourced dynamically from trusted supplier(s), this may make the supply route less predictable.
d) Provide security awareness, education, and training to suppliers and intermediate users to sensitize, educate, and implement security practices within the operational environment that protect the uses of the element.
e) Prefer suppliers who can support centralized and/or dispersed buying approaches upon request.

3.2.3 Supplier – General Requirements

a) None

3.2.4 Integrator – Technical Implementation Requirements

a) Limit disclosure of delivery process information.

[14] Dynamic sourcing is when varied sourcing techniques are used to acquire elements so that adversaries are not easily able to identify patterns of purchase.

b) Configure system and elements as well as items delivered as part of support and maintenance activities to conceal the uses of the element (e.g., disable or redirect "phone home" functions).
c) Limit disclosure of testing methods and procedures, test data, and communication routes by which such data is distributed, analyzed, and reported.

3.2.5 Supplier – Technical Implementation Requirements

a) Limit disclosure of delivery process information.
b) Configure delivered elements to conceal the uses of the element (e.g., disable or redirect "phone home" functions).
c) Limit disclosure of testing methods and procedures, test data, and communication routes by which such data is distributed, analyzed, and reported.

3.2.6 Integrator - Validation and Verification Requirements

a) Perform technical and procedural audits of mechanisms used to shield the uses of the element.
b) Employ Red Team approaches to identify potential pathways or opportunities for adversaries to exploit deficits or weaknesses in supply chain processes that would result in the exposure of the uses of the element.
c) Employ operational security tactics, techniques, and procedures to reinforce and extend the range of protections afforded to information shared with potential COTS suppliers as well as contracted suppliers, to sustain and enhance the confidentiality of element uses.

3.2.7 Supplier – Validation and Verification Requirements

a) None

3.2.8 Acquirer - Validation and Verification Activities

a) Review integrator's processes and procedures aimed at limiting exposure of system and elements uses.

3.3: Incorporate Supply Chain Assurance in Requirements

Protect against supply chain threats by employing an organization-defined list of requirements to protect against supply chain threats as part of a comprehensive defense-in-breadth information security strategy. Operational requirements, technical requirements, and mission/business rules must include requirements for supply chain assurance. These additional requirements will help ascertain that acquirers have considered and articulated their needs for supply chain assurance to their integrators and suppliers. These requirements should aid in reducing opportunities for unauthorized exposure or access of critical elements or processes.

3.3.1 Acquirer - Programmatic Activities

a) Categorize the information system and the information processed, stored, and transmitted by the system based on an impact analysis.[15] In the security control SA-12, "Supply Chain Protections," NIST SP 800-53, Rev. 3, specifies that information systems categorized at the FIPS 199 high-impact level be protected against supply chain threats.
b) Develop supply chain-related requirements that specify a baseline of security controls[16] to be implemented by the acquirer and the integrator. Incorporate supply chain risk considerations and assessments in all management, operational and technical requirements and mission/business processes to protect elements, processes, requirements, and acquirer mission/business practices against compromise. Work with stakeholders to clarify risks and threats to missions.
c) Promulgate acquisition strategy and procurement documents that incorporate specific requirements for the protection of critical supply chain elements processes, systems, and information. See other key practices for examples of requirements.
d) Protect requirements and supporting documentation from exposure or access that could result in the loss of the confidentiality, integrity, or availability of the elements through a supply chain-related compromise.

3.3.2 Integrators - General Requirements

a) Incorporate supply chain risk considerations and assessments in all management, operational and technical requirements and business processes to protect elements, processes, requirements, and acquirer business practices against compromise of confidentiality, integrity, or availability. Work with stakeholders to clarify risks and threats to missions.
b) Protect requirements and supporting documentation from exposure or access that could result in the loss of the confidentiality, integrity, or availability of the elements and systems through a supply chain-related compromise.

3.3.3 Suppliers - General Requirements

a) None

3.3.4 Integrators - Technical Implementation Requirements

a) Define technical specifications derived from operational requirements to include technical measures to protect supply chain activities including system and element production, assembly, packaging, delivery, testing, and support to understand, evaluate, and minimize opportunities for unauthorized exposure of or access to critical elements or processes that could result in a compromise.

[15] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, provides security categorization guidance for non-national security systems.
[16] NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, provides guidance for selecting and specifying security controls for information systems.

b) Apply identity management, access controls, and configuration management to the requirements process to ensure the confidentiality, integrity, and availability of requirements and supporting data, information, and requirement development tools.
c) Monitor and reassess evolving technical requirements and adjust requirements for protection of critical elements and processes throughout the element's life cycle.
d) Safeguard requirements, documentation, identities of participants in system development, customers, deliveries, etc., through appropriate information security mechanisms.
e) Experiment, simulate, model, and assess potential adversary attacks on the requirements levied upon the system/element or supply chain process to discover additional susceptibilities or vulnerabilities in the acquisition strategy, procurement process, or customer.
f) Verify through manual review, acceptance testing, or other quality assurance procedures that elements and components comply with standards and specifications.

3.3.5 Suppliers - Technical Implementation Requirements

a) Provide documentation, where available, of technical specifications derived from operational requirements to include technical measures to protect supply chain activities including element production, assembly, packaging, delivery, testing, and support to understand, evaluate, and minimize opportunities for unauthorized exposure of or access to critical elements or processes that could result in loss or compromise.

3.3.6 Integrators - Validation and Verification Requirements

a) Enforce information security requirements, including configuration management, on all critical data and information including the identity information associated with the development, refinement, and final publication of requirements.
b) When feasible, ascertain that the system/element "as produced is as designed, and as received is as produced."
c) Periodically assess the potential exposure of critical element requirements and exploit such information for access to elements or processes.
d) Assess supply chain activities that could result in the loss or compromise of the requirement or the element.

3.3.7 Suppliers - Validation and Verification Requirements

a) Provide documentation that the element "as produced is as designed, and as received is as produced." For example, compare the blueprint of the device with the physical device to find alterations.

3.3.8 Acquirer - Validation and Verification Activities

a) Audit and enforce integrator's organizational procurement practices associated with the development, refinement, and final publication of requirements.
b) Validate that the system/element "as produced is as designed, and as received is as produced."
c) Verify that supply chain requirements contained in the procurement contract have been met.

3.4: Select Trustworthy Elements

Elements may be assigned varying degrees of criticality depending on the purpose and use of each element. During their life cycle, elements may be subject to intentional or unintentional vulnerabilities, or may be subject to counterfeiting. Examine each element, not just the supplier, to determine element trustworthiness (that it is unlikely to have unintentional or intentional exploitable vulnerabilities, and that it is the element that was expected and not a counterfeit).

3.4.1 Acquirer – Programmatic Activities

a) Define and document acquisition processes by which elements are selected for use in systems and integrate these into the organization's operational practices, acquisition strategies, and procurement activities. Specify use of genuine and tested elements in contract documents.
b) For those cases when gray market elements are found in the supply chain, define and document procurement and maintenance processes for making decisions regarding keeping or disposing of these gray market elements, and for how to integrate them, after careful consideration, should a decision be made to use them.
c) Consider placing elements in escrow and not (fully) paying for those elements until verification is complete.

3.4.2 Integrators – General Requirements

a) Define and implement processes by which elements are selected for use in systems. Specify use of genuine and tested elements.
b) When gray market elements are found in the supply chain, notify the acquirer immediately. Work with the acquirer to decide whether to keep or dispose these elements and how to integrate them, should a decision be made to use them.
c) Establish an adequate supply of trusted spare and maintenance parts for well beyond the life span of the element.
d) For critical elements/services, determine the specific source of the element/service, not merely a corporate or organizational identity (most organizations are composed of different organizational entities whose trustworthiness is highly variable).
    - Ensure that practices (including product and personnel practices) have been put in place in the supplier organizational entity to

deliver elements/services with necessary confidentiality, integrity, and availability.
- For critical elements, consider using pre approved sources (e.g., trusted foundry/trusted integrated circuits for elements containing integrated circuits).

3.4.3 Suppliers – General Requirements

a) Define and implement processes by which elements are selected for use in systems. Specify use of genuine and tested elements.
b) Limit entrance of gray market items into the supply chain. If they have entered the supply chain, notify the acquirer immediately.

3.4.4 Integrators – Technical Implementation Requirements

a) Use or leverage any existing prequalified product lists (e.g., lists available from GSA, DHS, or internal integrator list) for identifying elements. If applicable, require elements to have certifications and validations such as Common Criteria, FIPS 140-2 validation, Security Content Automation Protocol (SCAP), and Federal Desktop Core Configuration (FDCC).
b) Determine and document the presence of abused behaviors or design deficits or weaknesses that could become vulnerabilities if exploited. For example, "call home" functionality in systems/elements can be dangerous, as is a default password that does not require change before use.
c) Use a variety of testing techniques to verify the trustworthiness of a system/element. Some of these techniques are further described in the key practice on testing, Section 3.11**.**
d) Consider placing elements in escrow and not (fully) paying for those elements until verification is complete.
e) If gray market items have entered the supply chain, they may provide an additional opportunity for subversion. Take actions to reduce such risks (e.g., additional verification, searching for malware, verifying firmware patches, comparison with known good products, and establishing larger stockpiles of spares).
f) Review elements to determine if source information matches that found on the approved products lists, and whether ownership has changed since its approval.

3.4.5 Suppliers – Technical Implementation Requirements

a) Identify, determine, and document the presence of easily abused behaviors or design deficits or weaknesses that could become vulnerabilities if exploited.
b) Use a variety of testing techniques to verify the trustworthiness of an element. Some of these techniques are further described in the key practice on testing, Section 3.11.
c) Provide elements "secured by default" at a level appropriate to the requirements of the acquiring organization.
d) Issue elements in a manner that facilitates proof of authenticity verification by the acquirer.

3.4.6 Integrators – Validation and Verification Requirements

a) Examine the element to ensure that it is new, that it was specified in requirements, and that all associated licenses are valid.
b) Identify past vulnerabilities in elements to determine if they have been addressed and what they indicate about the strength of the elements security.
c) Identify past vulnerabilities in processes used to produce elements to determine what they indicate about the strength of the elements security.
d) Implement a third-party assessment process for acceptance testing to ensure elements are genuine.

3.4.7 Suppliers – Validation and Verification Requirements

a) Develop a quality assurance statement or certification. Develop a description of the quality assurance processes employed**.**

3.4.8 Acquirer – Validation and Verification Activities

a) Examine the element to ensure that it is new, genuine, and tested, that it was specified in requirements, and that all associated licenses (including support agreements) are valid.
b) Review integrators' quality assurance processes to ensure compliance with requirements, Federal Procurement Policy, and Federal Acquisition Regulation (FAR).
c) In case gray market elements have entered the supply chain, employ additional acceptance testing to these elements to validate that they are performing as expected and do not introduce additional vulnerabilities.
d) Share results of assessments with others within the organization that are acquiring the same elements or using the same suppliers.

3.5: Enable Diversity

Element and supply chain diversity can increase robustness against attack by reducing the likelihood or consequences of attack. Diversity helps to counter a large impact from an attack on ubiquitous elements or processes. An attack is less likely to succeed if diversity is implemented. Diversity will help to ensure availability of required elements and continued supply in the event of compromise to the system/element.

3.5.1 Acquirer - Programmatic Activities

a) Develop procurement documents that require the use of government, international, or national standards where practical and feasible in order to make the elements replaceable with similar elements developed in compliance with the same standards in case the original supplier is unavailable.
b) Develop organizational policy and procedures that:
    - Consider an assessment of potential supply chain risks prior to making decisions restricting or limiting diversity of elements or suppliers.

        - Such assessments should discuss pros and cons of exposure of elements or supplier's/integrator's vulnerabilities and opportunities for exploitation based on known adversarial tactics, techniques, procedures, or tools, so that they could be mitigated through diversifying elements or the supply chain.
    - Identify cases where a standard configuration may reduce costs, but can increase risks due to known adversary tactics, techniques, and procedures.
c) Document the risk-based decisions in the system security plan taking above concerns into consideration.

3.5.2 Integrators - General Requirements

a) Conduct an assessment of the potential supply chain risks prior to making decisions restricting or limiting diversity of elements or suppliers, including legacy suppliers.
    - Such assessments should discuss pros and cons of exposure of suppliers or elements deficits, weaknesses, faults, vulnerabilities, and opportunities for exploitation based on known adversarial tactics, techniques, procedures, or tools, so that they could be mitigated through diversifying elements or the supply chain.
    - Identify cases where a standard configuration may reduce costs, but can increase risks due to known adversarial tactics, techniques, and procedures.
    - Document risk-based decision taking above concerns into consideration.
b) Consider using more than one implementation or configuration of both the supply chain and the element/system.
c) Implement diversity of supply and suppliers to ensure continuity of business operations.

3.5.3 Suppliers- General Requirements

a) Document diversity of suppliers to facilitate a change to alternative suppliers when the original supplier is unavailable.
b) Consider documenting alternative implementations of supplied elements including relative strengths and weaknesses of alternative elements, element designs, and element processes (including supplier business practices), as well as deficits, weaknesses, faults, or vulnerabilities.

3.5.4 Integrators - Technical Implementation Requirements

a) Perform assessments of alternative implementations of required functionality in elements to assess deficits, weaknesses, faults, or vulnerabilities. Document relative strengths and weaknesses of alternative elements, element designs, and element processes.
c) Consider using more than one implementation or configuration of both the supply chain and the element.
b) Consider using paired development for both systems and elements.

3.5.5 Suppliers - Technical Implementation Requirements

a) None.

3.5.6 Integrators - Validation and Verification Requirements

a) Review and evaluate the system/element criteria and decision outcomes for diversity choices.
b) Model, simulate, test, and evaluate the supply chain risks prior to decisions to limit the diversity of system/elements or suppliers.

3.5.7 Suppliers - Validation and Verification Requirements

a) None.

3.5.8 Acquirer - Validation and Verification Activities

a) Review and evaluate the application of criteria and decision outcomes for diversity choices against contractual requirements.

3.6: Identify and Protect Critical Processes and Elements

The purpose of identifying critical processes and elements is to allocate limited resources in an effective manner to protect the confidentiality, integrity, and availability of the information systems comprised of those elements throughout the elements system development life cycle (SDLC). In this key practice, the term *processes* encompasses all instances of an element or a system executing instructions concurrently as it is developed and operated. The failure modes and effects of various processes and elements must be understood; those processes and elements that present intolerable consequences for a system or mission must be protected. As the information system design is developed and refined, analyze it to identify the elements that could cause mission failure or compromise security.

3.6.1 Acquirer –Programmatic Activities

a) Define criteria for identifying a critical process or element for the specific system. The criteria should include:
    - Thresholds beyond which the degradation of processes and elements becomes unacceptable due to the impact on mission performance;
    - Information shared by other acquirers and integrators regarding environmental constraints and associated vulnerabilities;
    - The degradation of processes and elements that results in extensive modification or replacement long before its expected retirement from service, based on mean-time-between-failures (MTBF) for hardware and based on the number of releases for software; and

- The exposure of processes or elements that enables the development of countermeasures or adversary tactics, techniques, or procedures that would reduce information system assurance.

b) Develop organizational procedures, procurement processes, and procurement requirements that encourage identification and protection of critical processes and elements.
c) Define standardized technical interfaces and process requirements to provide options for the modification of processes or modification/replacement of elements should a supply chain compromise occur. For example, a ubiquitous element that is sole-sourced, or has a standard or non standard application programming interface (API), presents an opportunity for a supply chain compromise.
d) Require documentation of tactics, techniques, procedures, and tools used to protect critical processes and elements from exposure or access throughout all life cycle phases.

3.6.2 Integrators – General Requirements

a) Implement awareness, education, and training for all personnel regarding the protection of critical elements.
b) Develop, document, and implement procedures and tools to protect critical processes and elements from exposure or access.

3.6.3 Suppliers -– General Requirements

a) Determine and document hardware failure rates and periodically verify these rates.
b) Determine and document critical numbers of software patches or the extent of releases that would leave software vulnerable.
c) Develop processes to utilize, where appropriate, practices to institute original equipment manufacturer, OEM, product and software validation tools that are non invasive and could detect counterfeits or product intrusions.

3.6.4 Integrators – Technical Implementation Requirements

a) Identify critical elements by examining the composition of the system elements to ensure that their combination will not compromise the defenses. Combining two elements, each of which is individually secure from attack, may result in a new vulnerability.
c) Use defensive design (see Section 3.7), configuration management (see Section 3.12), and test methods (see Section 3.11) to develop and implement a plan for program protection.
d) Develop techniques to protect the system and its elements from unauthorized exposure and access. Leverage technical, management, and operational controls (e.g., NIST800-53).

3.6.5 Suppliers – Technical Implementation Requirements

a) Use defensive design (see Section 3.7**)**, configuration management (see Section 3.12), and test methods (see Section 3.11) on elements.
b) Implement processes and techniques to protect the elements from unauthorized exposure and access. Leverage technical, management, and operational techniques where available, validations, and certifications (FIPS 140-2 for cryptographic modules, Anti-Tamper methods, and Common Criteria certification) as appropriate.

3.6.6 Integrators – Validation and Verification Requirements

a) Use threat analysis techniques (such as threat modeling) to examine the overall integrated system's vulnerabilities in relation to its elements.
b) Assess the effectiveness of protective measures against threat actors to gain access to processes, system, or elements. Measures of protective effectiveness include time delay, required level of effort by the adversary, or ease of detection.

3.6.7 Suppliers – Validation and Verification Requirements

a) Use threat analysis techniques (such as threat modeling) to examine the element's design vulnerabilities.
b) Assess the effectiveness of protective measures against threat actors to gain access to processes, system, or elements. Measures of protective effectiveness include time delay, required level of effort by the adversary, or ease of detection.

3.6.8 Acquirer – Validation and Verification Activities

a) Review the documentation describing the effectiveness of the protection of critical elements. This may include evaluating the design (to see if it is a defensive design) and test results.
b) Evaluate the effectiveness of protective measures adopted by the acquirer and integrator to protect the confidentiality, integrity, and availability of critical elements.

3.7: Use Defensive Design

Defensive design techniques can be applied by both integrators and suppliers to ensure the integrity of individual elements and systems composed of these elements. It is important to note that even when elements originate from trustworthy suppliers, these elements may still have intentional or unintentional vulnerabilities (in isolation or when combined). Therefore, defensive design techniques should be deployed by the integrator within their architecture/design processes to reduce risk or damage to elements and systems.

Defensive design is the supply chain practice that aims to:

1. Anticipate potential ways that an element or system could fail or be misused.
2. Design the element or system to:
    a. Make such failure or misuse difficult or impossible, or
    b. Minimize the negative consequences.

3.7.1 Acquirer – Programmatic Activities

a) Incorporate defensive design criteria in all technical requirements. These requirements should result in design options for elements, systems, and/or processes that protect mission capabilities, system performance, or element confidentiality, integrity, and availability.
b) Develop organizational procedures that require design processes to address protective or corrective options which either avoid mission interruption or permit graceful degradation of the system should the system be attacked or compromised.

3.7.2 Integrators – General Requirements

a) Prefer elements that use broadly adopted industry standards, making it more feasible to replace them.
b) Maintain appropriate privileges, separation of duties, chain of custody, and protection of sensitive data related to elements or systems during the development process. This includes when collaboration is required among acquirers, integrators, and suppliers.

3.7.3 Suppliers – General Requirements

a) Report to the acquirer on element vulnerabilities including those exposed by element maintenance changes, standard interface changes, patches, and upgrades.
b) Deliver, where appropriate, sufficiently robust elements that do not degrade in performance, even when out-of-bounds inputs are provided (where practicable).
c) If available, provide assessment results of potential failure modes and effects on various proposed element designs based on the application of observed adversary tactics, techniques, procedures, and tools.
d) Establish processes to identify individual products and notify the acquirer when open/gray market products are mixed with products from authorized distribution or OEMs.

3.7.4 Integrators – Technical Implementation Requirements

a) Limit the number, size, and privileges of critical elements.
b) Reduce complexity of design, production processes, and design implementation.
c) Use defensive functions—that is, system elements whose purpose is to defend other functions—to reduce opportunities to exploit supply chain vulnerabilities in an information system. Examples of appropriate functions include

encryption, access control, and identity management, used to protect the confidentiality, integrity, and availability of mission functions.

d) Isolate system elements (using techniques such as virtual machines, quarantines, jails, sandboxes, and one-way gateways) to reduce the damage one element can do to another.
e) Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements.
f) Include the ability to configure increased system or system element isolation, even if this reduces system capability (e.g., counter attacks until a patch is available).
g) Elements should withstand out-of-bounds inputs (e.g., excessive voltages, numbers out of range, and so on), so that they are harder to disable. This may be important even if the element inputs should have been filtered elsewhere, because this makes the system more resistant to subversion.
h) Include fail-over/redundant systems or system elements when possible and appropriate.
i) Make systems resilient in case of misuse by insiders. Examples of techniques to improve system resilience include limiting communications, implementing communications within a contained area, limiting network port access, and implementing late or temporary binding techniques so connections can be quickly changed.
j) Use FIPS 140-2-validated cryptographic modules (in motion and at rest) and anti-tamper (including tamper-resistant and tamper-evident) mechanisms to counter theft and subversion (including auto-destruction if tampering is detected).
k) Test for security compliance on both ends of interfaces. One approach for testing is to replace a system element implementation with another implementation. Standardized interfaces facilitate the expanded use of test suites, potentially increasing the breadth of testing that can be done.
l) Implement hardware and software design using programming languages that avoid inherently insecure coding constructs to reduce the likelihood of weaknesses and supply chain-related compromise.
m) Enable compiler warnings *early* in development, and fix what is found. If compiler warnings are not enabled early, it is often excessively expensive to fix what is found later.
n) Identify and implement interface standards wherever practical to promote system and element sustainability and element reusability.
o) Develop processes to utilize, where appropriate, practices to institute OEM product and software validation tools that are non invasive and could detect counterfeits or product intrusions.

3.7.5 Suppliers – Technical Implementation Requirements

a) None.

3.7.6 Integrators – Validation and Verification Requirements

a) Use threat assessment techniques and information to determine if the proposed design alternatives meet defensive design criteria.

b) Verify that element's performance does not degrade or cause system failure even when out-of-bounds inputs are provided (where practicable).
c) Perform assessments of potential failure modes and effects on various proposed element designs based on the application of hypothesized or observed adversary tactics, techniques, procedures, and tools.
d) Assess opportunities for introduction of weaknesses and vulnerabilities systems and in elements as a result of different implementations of standards.
e) Test for compliance on both ends of an interface. One approach for testing is to replace a system element implementation with another implementation. Standardized interfaces facilitate the expanded use of test suites, potentially increasing the breadth of testing that can be done.
f) Develop technical and nontechnical techniques to expose or access systems or elements by exploiting interface standards.
g) When collaboration is required among acquirers, integrators, and suppliers evaluate implementation of information security, information assurance, and physical security that supports this collaboration.

3.7.7 Suppliers – Validation and Verification Requirements

a) None.

3.7.8 Acquirer – Validation and Verification Activities

a) Monitor, evaluate, test, and Red Team software and hardware implementation of designs for weaknesses and vulnerabilities; provide feedback to integrators and suppliers on findings, and work with them as they develop solutions and mitigating strategies.
b) Consider use of third parties to evaluate and test elements when those capabilities do not exist in-house.

3.8: Protect the Supply Chain Environment

Acquirers and integrators should employ adequate methods to prevent unauthorized or unmonitored access to their processes and environment including those used for research and development (R&D), test and evaluation (T&E), production, assembly, distribution, training, and logistics. Many processes and environments are highly distributed (logically and physically) and globalization is making such distributed approaches increasingly common. Failure to control physical or logical access to the acquirer, integrator or supplier environment may result in the sabotage of systems, elements or processes, the introduction of counterfeits or malware, the theft of critical materials and information (hardcopy or electronic data), or the subversion of systems in which the elements are embedded. Adequate protection should be determined, by the acquirer and integrator, based on threat and risk to the acquirer's mission. Acquirer and integrators should apply the protective measures discussed in this section to the critical system, element or process as discussed in Section 3.6**.**

3.8.1 Acquirer - Programmatic Activities

a) Establish and include in procurements requirements the need for intellectual property security, physical, information system security, and personnel security

necessary and sufficient to minimize unauthorized exposure of access to systems, elements, supply chain processes, and sensitive technical or mission/business process information of the element(s) and system(s) into which it is embedded.

3.8.2 Integrators - General Requirements

a) Document and demonstrate the implementation of physical security requirements throughout the development of the element including research, design/development, production, assembly, packaging, test, delivery, and support.
b) Demonstrate that a mix of personnel, physical, and logical access controls are implemented that provide a level of protection commensurate with the sensitivity/criticality of the services provided or the elements procured.

3.8.3 Suppliers - General Requirements

a) None.

3.8.4 Integrators - Technical Implementation Requirements

a) Implement written, repeatable processes for the purchasing, receipt, and delivery of materials for physical element delivery.
b) Designate and document authorized, where relevant, purchasers/delivery personnel for physical product delivery.
c) Use two-person (party) review for all orders and shipments, and the comparison of deliverables and receivables to requisition/purchase orders for accuracy of physical product delivery (an optimal practice may be the selection of two individuals from separate departments or duty areas).
d) Maintain documentation of individuals who were in possession of an element throughout purchasing, shipping, receiving, and transfer activities including records of reviewer's signatures for comparison for physical product delivery
e) Use secure storage (i.e., locking file cabinets on the integrator premises), where relevant, for all purchase order/delivery authorizations for physical product delivery.
f) Implement security audits and controls. Maintain a record/log of security related events or breaches. Notify the acquirer of any logged security events/breaches within an agreed to amount of time. Specific guidance on security events/breaches is provided in NIST SP 800-61, Computer Security Incident Handling Guide.

3.8.5 Suppliers - Technical Implementation Requirements

a) None

3.8.6 Integrators - Validation and Verification Requirements

a) Conduct inspection and acceptance testing of incoming items to detect evidence of tampering for physical product delivery.
b) Monitor and audit the developmental systems to detect malicious activity or surveillance. For example, in the systems integration development environment use intrusion detection/prevention/protection systems, both host-based and network-based.

3.8.7 Suppliers - Validation and Verification Requirements

a) None.

3.8.8 Acquirer - Validation and Verification Activities

a) Ensure integrators assess known adversary tactics, techniques, and procedures, and tools against physical, information security and information assurance, and personnel security practices employed to protect the supply chain environment.
b) Ensure integrators evaluate any alternative tactics, techniques, and procedures, and tools that may be employed which might degrade or compromise current physical, operational, and industrial security, information security and information assurance, and personnel security practices employed to protect the supply chain environment

3.9: Configure Elements to Limit Access and Exposure

Elements may include functionality that is not necessary to perform a particular mission. This is particularly common for COTS and in some cases GOTS elements, because COTS elements are designed to support multiple purposes. Some of this unnecessary functionality may permit unauthorized access or exposure of the system. NIST SP 800-70 Rev. 1 “National Checklist Program for IT Products – Guidelines for Checklist Users and Developers” provides guidelines on security configuration checklists (also called a lock down, hardening guide, or bench mark). A checklist is a series of instructions for configuring a product to a particular operational environment.

3.9.1 Acquirer – Programmatic Activities

a) Require integrators and suppliers to deliver elements with maximum security configurations.
b) Require elements to be configured to limit access and exposure.

3.9.2 Integrators – General Requirements

a) Deliver elements with maximum security configurations.

3.9.3 Suppliers – General Requirements

a) Provide elements with maximum security configurations.

3.9.4 Integrators – Technical Implementation Requirements

a) Use configuration documents that describe how to configure COTS and GOTS elements to limit unnecessary functionality or increase security. These include NIST-hosted configuration checklists, DISA Security Technical Implementation Guides (STIGs), and NSA Security configuration guides.[17] Incorporate checklists as early in the element/system life cycle as possible, to avoid unnecessary or dangerous functionalities. Leverage vendor-provided checklists if those exist.
b) Disable or remove and require suppliers to disable or remove unused functions of a system element, such as "extras" or extensibility functions such as plug-ins. Note that some of these "extras" may be useful to a system's mission, and are not unused functions.
c) Where practical, test and deliver the system with debug options off, or make the debug capabilities inaccessible to unauthorized users. While "debug" options may be useful during development, it is recommended to turn this function off and remove all relevant information from the executable system, to avoid exposure of system information that could lead to compromise.

3.9.5 Suppliers – Technical Implementation Requirements

a) Provide configuration documents in prose and Security Content Automation Protocol (SCAP) consumable form that describe how to configure COTS elements to limit their functionality or increase their security, to avoid unnecessary or dangerous functionalities.[18]

3.9.6 Integrators – Validation and Verification Requirements

a) Assess the effectiveness of alternative configurations in protecting the confidentiality, integrity, or availability of elements, processes, systems, and information against known vulnerabilities.

3.9.7 Suppliers – Validation and Verification Requirements

a) None.

[17] To obtain the NSA Security configuration guides, go to: http://www.nsa.gov/ia/guidance/security_configuration_guides/. The NIST/DHS National Checklist Repository Program is located at the following URL: http://web.nvd.nist.gov/view/ncp/repository.
[18] For more information on SCAP see NIST SP 800-126, The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.0.

3.9.8 Acquirer – Validation and Verification Activities

a) Review test and evaluation results throughout the life cycle to ensure compliance with configuration requirements as defined within the program.

3.10: Formalize Service/Maintenance

Service and maintenance process begins when the element has been released to users for the first time. The set of system components are in place, the system has been tested and accepted for operational use, operators have been trained, and logistics support has been arranged. From that point on, the service has to be managed throughout the evolution of the element within the information system. This includes situations when an element has a long life span and requires multiple upgrades or spare parts. Upgrades and spare parts will be delivered during varying stages of the life cycle, which may provide opportunities for subversion through the supply chain. The service and support processes throughout the life cycle should limit opportunities and means for unauthorized access to or exposure of elements and operational processes.

This key practice applies to both the bounded operational system within the acquirers' environment which may require multi tiered-supplier operational support, as well as the outsourced operational information system provided by a service provider which is used remotely by the acquirer. ***For this practice, the service provider is considered a supplier.*** The integrator is considered a pre operational service provider within the system lifecycle and is not the focus of this key practice.

The maintenance security controls contained in NIST SP 800-53 provide a baseline of assurances that organizations should employ. The practices described below build on the maintenance security controls with emphasis on mitigating supply chain risk for those information systems categorized as a FIPS 199 high-impact system.

3.10.1 Acquirer – Programmatic Activities

a) Include procurement clauses to reduce supply chain risk in formal service and maintenance agreements with suppliers.
b) When acquiring OEM original equipment manufacturer(s) elements, including refurbished elements, establish a contractual relationship with the original manufacturer or originator that provides vetted, competent support where possible.
    - Where possible (including rapid acquisition), purchase only elements/services known to have been previously screened for supply chain risks (including counterfeits and subversion).
    - Consider advance purchase and inventory of spare parts while they are widely available and verifiable and can be installed by trained and knowledgeable authorized service personnel.
    - Consider supply chain risks when acquiring replacement components or field additions/modifications/upgrades, particularly if they do not go through traditional acquisition processes that examine SC risks.

- Perform a more rigorous SCRM review throughout the purchasing process when any affected elements are critical.

c) Prefer formalized service/maintenance agreement(s) where possible:
   - Maintenance personnel should meet certain criteria (see Section 3.10).
   - Use specified or qualified spare parts suppliers.
   - Report major changes in a maintenance organization's structure (e.g., physical move to a different location/off shoring, change in ownership, outsourcing, and changes in personnel).
   - Provide a complete record of changes performed during maintenance (e.g., audit trail or change log).
   - Independent review of changes made during maintenance.

d) Establish and implement agreements for competent and suitable support including refurbished and/or salvaged elements, when acquiring COTS and GOTS. Consider requiring the original manufacturer to certify the equipment as suitable.

e) Identify methods of verifying that service personnel are authenticated and authorized to perform the service work needed at the time.

f) Require supplier to identify the expected life span of the element to help acquirer plan for any migration that might be required in support of continued system and mission operations.

g) Require suppliers to purchase only elements/services known to have been previously screened for supply chain risks (including counterfeits and subversion) as much as possible.

h) Software is often not warranted. Some software suppliers may be willing to provide service/maintenance agreements such as service-level agreements, limited warranties, or a maintenance contract. Consider establishing such service agreements for critical software elements. For example, such agreements could include language that the supplier:
   - Repair any problem within a specified time if it is a common security weakness (such as the Open Web Application Security Project [OWASP] top ten [OWASP 2010] or the Common Weakness Enumeration [CWE 2008]) or incur a financial penalty.
   - Check for pre existing malware (e.g., using a virus checker or static analyzer tools) before accepting delivery. Where practical, perform checks after delivery of patches or later revisions/updates, and/or perform periodic checks.
   - If using third-party or open source software, update the software if vulnerabilities in that software are publicly disclosed and patches/updates are available.

j) Require training on original equipment manufacturer (OEM) procedures for acquiring secondary market (refurbished) items.

3.10.2 Integrators – General Requirements

a) None.

3.10.3 Suppliers – General Requirements

a) Avoid introducing new actors in maintenance activities where possible. (e.g., keep original manufacturers and/or OEM-authorized suppliers). If new actors must be added, require a vetting process for them before they are needed.
b) Examine organization and process certifications. Determine if the supplier is an authorized distributor/reseller/maintainer by the OEM to help determine risk (e.g., recipient may lose integrity/availability if it will not be serviced later, and if subverted, may lose confidentiality). This includes "gray market," potentially counterfeit, and potentially subverted elements.
c) Notify acquirer of any major changes in a maintenance organization's structure or process (e.g., physical move to a different location/off shoring, change in ownership, outsourcing, and/or changes in personnel).
d) Notify acquirer of any changes in element life span including end of life to enable the acquirer to plan for any migration that might be required in support of continued system and mission operations.

3.10.4 Integrators -– Technical Implementation Requirements

a) None.

3.10.5 Supplier – Technical Implementation Requirements

a) Provide maintenance personnel capable of meeting terms of contract.
b) Ensure remote maintenance is used only for approved purposes.

3.10.6 Integrators – Validation and Verification Requirements

a) None.

3.10.7 Suppliers - – Validation and Verification Requirements

a) Conduct additional manual review and inspection, as well as acceptance testing when refurbished or gray market items are permitted for use during initial procurement and continuing through operations and sustainment.
b) Evaluate changes in maintenance agreements (e.g., physical move to different location/off shoring, changes in ownership, outsourcing, and change in personnel) and manage risks associated with them.
c) Segregate the same elements coming in from different suppliers to ensure that if a particular order needs to be isolated, the elements from that order can be identified.

3.10.8 Acquirer -– Validation and Verification Activities

a) Conduct additional manual review and inspection, as well as acceptance testing when refurbished or gray market elements are permitted for use during initial procurement and continuing through operations and sustainment.
b) Review the suppliers' service and maintenance programs and procedures for compliance with contractual requirements.

c) Evaluate changes in maintenance agreements (e.g., physical move to a different location/off shoring, change in ownership, outsourcing, and changes in personnel) and manage risks associated with them.

3.11: Test Throughout the System Development Lifecycle

Testing is a critical practice used to ascertain that defensive measures have been deployed. The purpose of testing is to validate compliance with requirements, ascertain that the system behaves in a predictable manner under stress, and detect and classify weaknesses and vulnerabilities of elements, processes, systems, and information that flow through them.

The testing will help determine if remedial actions for vulnerabilities are required based on the environment and uses, and simulate potential attacks in controlled environments using multiple scenarios. Testing should be conducted in multiple contexts including the selection of COTS elements, integrating COTS and GOTS into larger systems, and accepting delivery of COTS, GOTS, custom elements, or open sources. This may be done at different points during the system or element life cycle including development and throughout operations.

Multiple types of testing should be used including manual review, fuzz testing, static analysis, dynamic analysis, and penetration testing. Manual review involves human review of design, architecture, code, processes, procedures, and other aspects of system development, integration, and operation, such as inspection and auditing of configuration. Fuzz testing provides invalid, unexpected, or random data as program input; failure helps to identify which piece of software might be failing. Static analysis is the use of automated tools to analyze: (1) elements (software and hardware) without executing them, (2) processes without actually exercising them, or (3) information that would flow through them. Dynamic analysis executes an element or process, or a simulation of it, with test input to determine if its results match expectations. Dynamic analysis can be used to evaluate elements in their environment. It is helpful for finding unintentional vulnerabilities that could compromise confidentiality, integrity, or availability. Dynamic analysis techniques include system modeling and simulation, functional and acceptance testing, network vulnerability analysis, network and Web application vulnerability scanning, and protocol analysis. Penetration testing involves humans or computing elements (enabled by tools) to execute or simulate attacks in controlled environments of one or more scenarios, to detect vulnerabilities needing repair.

3.11.1 Acquirer – Programmatic Activities

a) Develop a comprehensive testing policy and procedures that incorporate the testing practices described in this section.
b) Require implementation of manual review of operational and technical requirements and mandatory business practices (processes and rules). Include manual review where applicable, including during all milestone or “make

versus buy" decisions, design reviews, reviews of acquisition and procurement plans, and reviews of vulnerabilities in elements and processes.

c) Require that reviewers are qualified to identify vulnerabilities.
d) Require that fuzz testing include: environment variables, keyboard and mouse events, and sequences of APIs.
e) Require implementation of static and dynamic analysis for selected elements and processes (e.g., automated manufacturing/test processes and delivery mechanisms).
f) Require that penetration testing be a realistic simulation of the active adversary's known adversary tactics, techniques, procedures, and tools.
g) When practical, prefer static and dynamic analysis tools usage to evaluate potential critical system elements before: 1) making a make-buy decision; 2) selecting COTS/GOTS and/or open source elements; and 3) accepting COTS /GOTS, open source, or custom elements into the system.
h) State the conditions and criteria throughout the life cycle for physical and logical penetration testing of systems, elements, or processes.

3.11.2 Integrators – General Requirements

a) Perform manual review of elements, processes, and system to identify and remediate any weaknesses and vulnerabilities including peer reviews (e.g., walk-throughs and inspections) and comprehensive or sampled reviews. (Employ independent internal or external reviewers: external reviewers may be able to spot issues that people too close to the system cannot, and may have expertise that internal reviewers lack; internal reviewers may know key information that external reviewers do not.)
b) Use two-person control when performing custom development and integration of critical elements and performing critical processes. This may be implemented by paired development processes.
d) Apply static and dynamic analysis tools to potential system elements before: 1) making a make-buy decision; 2) selecting COTS/GOTS and/or open source elements; and 3) accepting COTS /GOTS, open source, or custom elements into the system.
e) Determine the conditions and criteria throughout the life cycle for physical and logical penetration testing of systems, elements, or processes.
f) Apply fuzz testing to assess robustness of code and aid in identification of defects.
g) Ensure that any new code extensions or customization is subject to the same rigorous set of testing as required of the supplier.

3.11.3 Suppliers – General Requirements

a) Perform manual review of sub systems, elements, and processes to identify and remediate any weaknesses and vulnerabilities; include peer reviews (e.g., walk-throughs and inspections) and comprehensive or sampled reviews.
b) Employ independent internal or external reviewers: external reviewers may be able to spot issues that people too close to the element or information system cannot, and may have expertise that internal reviewers lack; internal reviewers may know key information that external reviewers do not.
c) Apply fuzz testing to assess robustness of code and aid in identification of defects.

3.11.4 Integrators – Technical Implementation Requirements

a) Prepare personnel participating in manual reviews by reporting or demonstrating known adversary tactics, techniques, procedures, and tools for exploiting weaknesses or deficits in systems/elements, assemblies, information systems, or processes.
b) Apply fuzz testing to systems to identify high-level pointers to specific areas that might need in-depth testing by other means.
c) Apply static analysis tools to systems to: identify architecture, design, and implementation weaknesses, search for common security weaknesses (constructs) and vulnerabilities, search for virus/malware signatures (e.g., virus scanning), and identify failures to comply with standards.
d) Apply dynamic analysis tools to systems to: search for common security weaknesses (constructs) and vulnerabilities, and identify failures to comply with requirements.
e) Apply static and dynamic analysis tools to element/system processes to: identify vulnerabilities or weaknesses in processes (including gaps), and identify failures to comply with process requirements.
f) Enable optional compiler warnings (where practical) early in the code development process to identify weaknesses and reduce false alarms. Compilers used in software development include some static analysis capabilities, but remediating the software can become difficult if the warnings are not enabled early. An example is “-Wall” in the GNU Compiler Collection (GCC).
g) Develop and run both negative and positive tests – test that the system/element/process does not do what it should not do, as well as testing that it does what it is supposed to do.
h) Monitor for unexpected or undesirable behavior during tests. This could include network behavior (such as a surprise “call home” or opening of network port), file system behavior (such as reading or writing information in unexpected files/directories), race conditions, and deadlocks.

i) Protect accessing of test cases and results using digital signatures.

3.11.5 Suppliers – Technical Implementation Requirements

a) Apply fuzz testing to systems to identify high-level pointers to specific areas that might need in-depth testing by other means.
b) Apply static analysis tools against sub systems and elements to: identify architecture, design, and implementation weaknesses, search for common security weaknesses (constructs) and vulnerabilities, search for virus/malware signatures (e.g., virus scanning), and identify failures to comply with requirements.
c) Apply dynamic analysis tools to sub systems and elements to: search for common security weaknesses (constructs) and vulnerabilities, and identify compliance and non compliance with relevant standards.
d) Apply static and dynamic analysis tools to elements to: identify vulnerabilities or weaknesses in processes (including gaps), and identify failures to comply with process standards.
e) Enable optional compiler warnings (where practical) early in the code development process to identify weaknesses and reduce false alarms. Compilers used in software development include some static analysis capabilities, but remediating the software can become difficult if the warnings are not enabled early. An example is "-Wall" in the GNU Compiler Collection (GCC).
f) Develop and run both negative and positive tests – test that the system/element/process does not do what it should not do, as well as testing that it does what it is supposed to do.
g) Monitor for unexpected or undesirable behavior during tests. This could include network behavior (such as a surprise "call home" or opening of network port), file system behavior (such as reading or writing information in unexpected files/directories), race conditions, and deadlocks.

3.11.6 Integrators – Validation and Verification Requirements

a) Monitor and assess the implementation of systems and the results of manual review requirements to ensure compliance with laws, regulations, and policies and conformance to contract specifications or standards.
b) Assess testing results (from all types of testing) to identify additional vulnerabilities that may be exploited by threat actors, and report results of such assessments.

3.11.7 Suppliers – Validation and Verification Requirements

a) None

3.11.8 Acquirers – Validation and Verification

a) Incorporate testing results (from all types of testing) into the oversight of other supply chain practices.
b) Monitor and assess the implementation and the results of manual review requirements to ensure compliance with laws, regulations, and policies and conformance to contract specifications or standards.
c) Monitor and assess the implementation and the results of static and dynamic analysis.
d) Apply penetration testing to potential system elements before accepting the system.

3.12: Manage Configuration

As described in Draft NIST SP 800-126 *Guide for Security Configuration Management of Information Systems,* an information system is composed of many components (elements) that can be interconnected in a multitude of arrangements to meet a variety of business, mission, and information security needs. An information system is typically in a constant state of change in response to new or enhanced hardware, software, updates, patches, new security threats, etc. To ensure that the required adjustments to the security configurations do not adversely affect the information system, a well-defined security configuration management process is needed. Configuration management (CM) processes can be enhanced to reduce supply chain risks. When integrating a variety of elements into a system, the integrator should store elements and related configuration management information securely so that the information about elements is protected and managed throughout the integration and system deployment process. Given the importance of CM, any systems containing CM information should be sufficiently hardened, including against physical attacks.

3.12.1 Acquirer – Programmatic Activities

a) Incorporate supply chain mitigations and practices into existing organization configuration management policies and procedures.
b) Include provisions in contract documents and program plans requiring a Configuration Management Plan and that CM be applied to documentation developed or used within the element or system SDLC, including requirements and interface specifications, the elements including design libraries, tools including design tools and test tools, technical data including test data, and information on specific element and system SDLC processes.

3.12.2 Integrators – General Requirements

a) Protect information systems containing CM information against unauthorized exposure and access, including via physical and logical attacks.

b) Perform CM of documentation, COTS, GOTS, and custom system/element configurations in accordance with a CM Plan. Some of this configuration management may be done centrally (e.g., organization-wide to support a site license), while others might use a more local approach.
c) Maintain baseline throughout the life cycle. Require establishment and implementation of a policy to monitor and maintain a valid baseline. This includes covering spare parts and warehoused systems/elements.
d) Perform security assessments of the CM processes to attempt detection of ongoing attacks (including the CM systems).
e) Add configuration items (CIs) into the configuration management system when new elements are introduced to the supply chain.

3.12.3 Suppliers – General Requirements

a) Document CM of elements including details such as spare parts and warehoused systems/elements.
b) Provide documentation regarding element configuration baselines for components provided by suppliers.

3.12.4 Integrators – Technical Implementation Requirements

a) Back up information systems containing CM information, implement immutable chains (e.g., digital signatures proving a sequence of events), and deploy a recovery process when a CM information system is breached or unavailable.
b) Implement identification/authentication/authorization mechanisms to identify specific personnel (e.g., specific developers) involved in the administering of change to configuration items as well as the configuration management system. Consider using multifactor approaches, and role- and attribute-based mechanisms.
c) Implement least privilege that specifies who can view the information, change the information, what types of changes are allowed, and when these changes are allowed. For time limits, consider including revalidation, inactivity, and duration. Consider protecting specifications (including performance), designs, or implementations, to inhibit sharing them with unauthorized personnel.
d) Implement accountability for all changes in configuration items by recording the identity of each individual who is making a change, when each change was made, and exactly what the change was. This information should be authenticated such that it cannot be repudiated (digital signatures can be used to confirm this information). Ensure that audit logs are retained long enough to meet compliance requirements.
e) Enable the CM process to report, for a given specific result (e.g., a particular line of code), the change that produced that result including who made the

change, what change was made, and when it was made. This can be tied to original documented specifications, enhancements, or defect tracking systems. This is sometimes referred to as "annote" or "blame" functionality. Similarly, ensure that the CM process can report any and all changes made by a given individual.

f) Record location information of the actor making the change, and where it can be reliably obtained. Locations may be physical (e.g., geospatial) or logical (IP address).
g) Establish performance and sub-element baselines for the system and system elements. This helps detect unauthorized tampering/modification during repairs/refurbishing, as well as other activities such as auditing (including independent auditing). For example, consider using Radio Frequency (RF) interrogation of Integrated Circuits (IC), and compare those results to results from known and trusted ICs.
h) Integrate mechanism(s) to uniquely identify system-critical hardware elements such as a physical identifier or authenticator to the hardware. This makes unauthorized substitutions more detectable.

3.12.5 Suppliers – Technical Implementation Requirements

a) Establish configuration element baseline for elements. This helps detect unauthorized tampering/modification during repairs/refurbishing, as well as other activities such as auditing (including independent auditing). For example, consider using RF interrogation of ICs, and compare those results to results from known trusted ICs.
b) Integrate mechanism(s) to uniquely identify critical hardware elements such as a physical identifier or authenticator to the hardware. This makes unauthorized substitutions more detectable.

3.12.6 Integrators – Validation and Verification Requirements

a) Monitor and audit the CM systems to attempt detection of ongoing attacks. For example, use intrusion detection/prevention/protection systems, both host-based and network-based.
b) Perform compliance audit on CM processes and activities.
c) Perform security assessments of the CM processes (including the CM systems).

3.12.7 Suppliers – Validation and Verification Requirements

a) None

3.12.8 Acquirer – Validation and Verification Activities

a) Review acquirer's CM processes and activities.

b) Review integrator's completion of security assessments of the CM processes (including the CM systems).
c) Review integrator's monitoring and auditing of the CM systems to attempt detection of ongoing attack.

3.13: Consider Personnel in the Supply Chain

Personnel and their roles are critical for implementing a robust supply chain risk management (SCRM) capability. The personnel security controls contained in NIST SP 800-53 provides a baseline of personnel-related assurances that organizations should employ to protect their information and information systems. These controls include security awareness and training, and separation of duties which are critical for achieving SCRM. The practices described below build on those baseline NIST SP 800-53 personnel security controls with emphasis on people who implement supply chain processes for elements contained in applicable information systems.

3.13.1 Acquirer Programmatic Activities

a) Establish organizational policy and general contractual requirements to address personnel supply chain security awareness, education, and training throughout integrator and supplier organizations.
b) Define, design, specify, and require roles throughout the supply chain and system/element life cycle to limit opportunities and means available to individuals performing these roles that could result in adverse consequences.
c) Require supply chain security awareness, education, and training for acquirer personnel.
d) Employ consideration of suppliers past performance regarding personnel policies, procedures, and security practices as part of source selection requirements and processes.
e) Ensure there is no “single person point of failure” for key positions (including operations and maintenance) to reduce program impact if any particular key person departs.
f) Evaluate all positions for opportunities to expose or access elements, processes, systems, or information, including requirements.
g) Establish and enforce requirements for personnel security reviews and assessments for personnel employed by acquirers. These reviews and assessments should include personnel who have exposure or access to elements, element processes, or business activities that would allow an opportunity to apply technical knowledge or understanding of business processes to obtain unauthorized exposure of, or access to, elements or processes that could result in compromise or loss.

3.13.2 Integrator – General Requirements

a) Define, design, and implement roles throughout the supply chain and life cycle to limit opportunities and means available to individuals performing these roles that could result in adverse consequences.
b) Demonstrate that individuals are assigned throughout the supply chain and life cycle to roles in a manner that limits their opportunities or means to cause adverse consequences.
c) Conduct personnel security reviews and assessments. Include those personnel who have exposure or access to elements, element processes, or business activities that would allow an opportunity to apply technical knowledge or understanding of business processes to obtain unauthorized exposure of, or access to, elements or processes that could result in compromise or loss of confidentiality, integrity, or availability.
d) Conduct supply chain security awareness, education, and training for key personnel.
e) Document evidence of separation of duties applied to limit opportunities and means to cause adverse consequences, across the supply chain and the element life cycle.

3.13.3 Supplier – General Requirements

a) Conduct supply chain security awareness, education, and training for personnel involved in supply chain-related activities.

3.13.4 Integrator – Technical Implementation Requirements

a) Implement identity management, access controls, and process monitoring to permit timely detection and classification of anomalous behaviors that may result in adverse consequences for both physical and logical access.

3.13.5 Supplier – Technical Implementation Requirements

a) Demonstrate that identity management, access controls, and process monitoring facilitate timely detection and classification of anomalous behaviors that may result in adverse consequences for both physical and logical access.

3.13.6 Integrator - Validation and Verification Requirements

a) Evaluate key personnel for competency (i.e., possess knowledge, skills, and abilities to perform assigned tasks).
b) Re evaluate key personnel on a periodic basis or upon occurrence of specific significant events in support of systems and mission requirements.

c) Continuously monitor internal controls addressing allocation of tasks and activities to roles.
d) Test internal controls for ability to detect anomalous behavior and facilitate timely intervention to prevent or reduce adverse consequences.

3.13.7 Supplier - Validation and Verification Requirements

a) Demonstrate effective implementation of separation of duties/roles.
b) Demonstrate ability to intervene in a timely manner to prevent or reduce adverse consequences.

3.13.8 Acquirer - Validation and Verification Activities

a) Examine the hiring and personnel policies and practices of integrators and potential suppliers to assess the strengths or weaknesses of their personnel security policies and procedures.
b) Review personnel security policies and practices of all integrators.
c) Evaluate acquirer and integrator positions for opportunities to expose or access elements, processes, systems, or information, including requirements.
d) Assess the effectiveness of integrator and supplier identity management and access control policies, procedures, and practices in limiting exposure of or access to elements or element processes.
e) Continuously monitor acquirers' and integrators' internal controls over allocation of tasks and activities to roles.
f) Test acquirers' and integrators' internal controls for effectiveness in detection of anomalous behavior and timely intervention to prevent or reduce adverse consequences.

3.14: Promote Awareness, Educate, and Train Personnel on Supply Chain Risk

A strong supply chain risk mitigation strategy cannot be put in place without significant attention given to training organizational personnel on supply chain policy, procedures, and applicable management, operational, and technical controls and practices. NIST SP 800-50 *Building an Information Technology Security Awareness and Training Program,* provides guidelines for establishing and maintaining a comprehensive awareness and training program. This practice focuses on supply chain-specific awareness, education, and training activities and requirements.

3.14.1 Acquirer – Programmatic Activities

a) Develop a comprehensive awareness and training program that promotes the organization's SCRM policy and procedures.
b) Require SCRM awareness training for all acquirer and integrator personnel involved in requirements, acquisition, and procurement activities.

c) Train personnel with purchase requisition authority or a government purchase card (GPC) regarding organizational SCRM policy and procedures.
d) Define processes by which general supply chain information will be collected, lessons learned extracted, and shared between acquirers, integrators, and suppliers as scoped within the contract.
e) Provide training to appropriate staff on Original Equipment Manufacturer (OEM) procedures for acquiring secondary market (refurbished) items, to ensure that secondary market items are adequately supported and maintained. Incorporate training from authoritative OEM materials.

3.14.2 Integrators – General Requirements

a) Provide supply chain risk awareness/education/training to help integrator personnel identify deficits/weaknesses and faults/vulnerabilities in the supply chain, including both opportunities for harm and the means (tools, techniques, and procedures).
b) Share relevant SCRM information across the life cycle, including with personnel who are assigned a new role (e.g., due to a change in the life cycle phase) and with new personnel. Note that transitioning a system to an organization operating the system and any associated suppliers often involves a change in personnel.
c) Provide training to appropriate staff on OEM procedures for acquiring secondary market (refurbished) items, to ensure that secondary market items are adequately supported and maintained. Incorporate training from authoritative OEM materials.
d) Educate and train system administrators and users in what information should be kept secure (for confidentiality, integrity, and availability) so that supplier intermediaries are not revealed.

3.14.3 Suppliers – General Requirements

a) Provide awareness training to supplier staff on their supply chain roles, responsibilities, policies, and procedures.
b) Provide supply chain risk awareness/education/training to help personnel identify deficits/weaknesses and faults/vulnerabilities in the supply chain, including both opportunities for harm and the means (tools, techniques, and procedures).

3.14.4 Integrators – Technical Implementation Requirements

a) Train receiving personnel (such as technical personnel, equipment specialists, and item managers) on correct processes for receipt of elements/services (including spare parts), including any known parts anomalies (which may indicate counterfeits, subversion, or quality issues).

3.14.5 Suppliers – Technical Implementation Requirements

a) Develop policy and procedures that require receiving personnel (such as technical personnel, equipment specialists, and item managers) to be trained on

organizational processes for receipt of elements/services (including spare parts), including any known parts anomalies (which may indicate counterfeits, subversion, or quality issues).

3.14.6 Integrators – Verification and Validation Requirements

a) Provide periodic documentation demonstrating the implementation of a comprehensive SCRM training program.
b) Provide periodic update on status of personnel SCRM training in support of contractual requirements.

3.14.7 Suppliers – Verification and Validation Requirements

a) Document how SCRM awareness is implemented within the supplier organization.

3.14.8 Acquirer – Validation and Verification Activities

a) Monitor and review acquisition/procurement documents to ensure requirements for awareness, education, and training are included.
b) Review integrator performance of supply chain risk awareness, education, and training against requirements.
c) Assess integrator effectiveness of supply chain risk awareness, education, and training.

3.15: Harden Supply Chain Delivery Mechanisms

Ensure that element delivery mechanisms (both physical and logical) used by acquirers/integrators/suppliers protect the confidentiality, integrity, or availability of systems and elements delivered through the supply chain. Ensure that the delivery mechanisms do not provide opportunities for unauthorized access to the element and system, or exposure of the element or system, and information about their uses. Unauthorized access may include unauthorized modification (including substitution and subversion) or redirection of elements by active adversaries to an alternate location. This practice includes the delivery of system elements to integrators, delivery of the system itself to acquirers, and system maintenance (including repair and delivery of replacement parts or software). This practice also includes inventory management for the system and its elements.

3.15.1 Acquirer - Programmatic Activities

a) Require systems/elements to be incorporated into the organization’s inventory management system.
b) Examine organization’s inventory management policies and processes to ensure they include how to request replacements, appropriate stocking (including spare locations and protection of spares), receipt policies (to know who the inventory should go to, when it arrives, who handled it, where it is

located, and if the received inventory is reconciled to what was ordered), and inventory counting/accounting policies.

c) Determine what system and system element replacements will be needed, when, where, and how quickly. Some critical element spares may need to be stored near or with systems so that they can be rapidly replaced. For organizations using just-in-time delivery, ensure that the system/element will be delivered in time even in a stressed/emergency environment.

d) Require education and training for acquirer personnel on inventory management policies and processes.

3.15.2 Integrators - General Requirements

a) Establish processes for the system or element to be delivered when it is needed:
   - Modify the delivery path so that it is difficult to prevent delivery (e.g., via sabotage).
   - Have multiple delivery paths, in case a delivery path is unavailable or compromised.
   - Use a variety of vetted delivery paths.

b) Establish a minimum baseline for supply chain delivery, processes, and mechanisms. Where appropriate, use trusted contacts and ship via a protected carrier (such as U.S. registered mail, using cleared/official couriers, or a diplomatic pouch). Protect the system/element while storing before use (including spares).

c) Design delivery mechanisms to avoid exposure or access to the system and element delivery processes, and use of the element during the delivery process.

d) Implement delivery processes for the intended logical and physical transfer and receipt of elements to be done by authorized personnel.

e) Require education and training for personnel on inventory management policies and processes.

f) Use nondestructive techniques or mechanisms to determine if there is any unauthorized access throughout the delivery process.

3.15.3 Suppliers - General Requirements

a) Establish processes for the element to be delivered when it is needed:
   - Modify the delivery path so that it is difficult to prevent delivery (e.g., via sabotage).
   - Have multiple delivery paths, in case a delivery path is unavailable or compromised.
   - Use a variety of vetted delivery paths.

b) Establish a minimum baseline for supply chain delivery, processes, and mechanisms. Where appropriate, use trusted contacts and ship via a protected carrier (such as U.S. registered mail, using cleared/official couriers, or a diplomatic pouch). Protect the system/element while storing before use (including spares).

c) Implement delivery processes for the intended logical and physical transfer and receipt of elements to be done by authorized personnel.

d) Provide documentation of any nondestructive techniques or mechanisms to determine if there is any unauthorized access throughout the delivery process.

3.15.4 Integrators - Technical Implementation Requirements

a) Use and check difficult-to-forge marks (such as digital signatures and hologram tags) for all critical elements.
b) Use anti-tamper mechanisms for prevention and discovery, including tamper-resistant and tamper-evident packaging (e.g., tamper tape or seals). These must not be easy to remove and replace without leaving evidence of such activity.
c) Stipulate assurance levels and monitor logical delivery of products and services, requiring downloading from approved, verification-enhanced sites. Consider encrypting elements (software, software patches, etc.) in transit (motion) and at rest throughout delivery. Mechanisms that use cryptographic algorithms must be compliant with NIST FIPS 140-2.
d) Include in inventory management policies and processes how to request replacements, appropriate stocking (including spare locations and protection of spares), receipt policies (to know who the inventory should go to, when it arrives, who handled it, where it is located, and if the received inventory is reconciled with what was ordered), and inventory counting/accounting policies.
e) Consider using multiple sources and then comparing them, to see if the elements have unexplained differences (e.g., in appearance, performance, or software hash codes). Ensure that the multiple sources are truly diverse.

3.15.5 Suppliers - Technical Implementation Requirements

a) Use and check difficult-to-forge marks (such as digital signatures and hologram tags) for all critical elements.
b) Document any anti-tamper mechanisms used for prevention and discovery, including tamper-resistant and tamper-evident packaging (e.g., tamper tape or seals). These must not be easy to undetectably remove and replace.
c) Document and monitor logical delivery of elements, requiring downloading from approved, verification-enhanced sites. Consider encrypting elements (software, software patches, etc.) in transit (motion) and at rest throughout delivery. Mechanisms that use cryptographic algorithms must be compliant with NIST FIPS 140-2.
e) Document and resolve potential threat actor attacks on delivery mechanisms to estimate and evaluate potential loss or compromise of confidentiality, integrity, or availability of elements.

3.15.6 Integrators - Validation and Verification Requirements

a) Use modeling, simulation, tests, exercises, drills, war games, or “Red Team” exercises to assess supply chain delivery processes to ascertain the susceptibility and vulnerability of elements to sabotage, subversion, or compromise during delivery.
b) Perform physical and information security reviews of supply chain mechanisms used by suppliers to assess the effectiveness of measures intended to reduce opportunities for exposure of or access to elements, processes, or information regarding elements or processes.

3.15.7 Suppliers - Validation and Verification Requirements

e) None

3.15.8 Acquirer - Validation and Verification Activities

a) Verify that the supplier/integrator has documented processes for hardening of delivery mechanisms when required, use of protective physical and logical packaging approaches for systems/elements and associated technical or business process information, and protection of element processes throughout the system's/element's life cycle.
b) Review and make recommendations regarding the training of supplier personnel in methods and performance of tasks to harden supply chain delivery mechanisms.
c) Verify that delivery processes ensure that the intended transfer and receipt of elements and services will only be done by authorized personnel. (ANSI/NASPO-SA-2008).
d) Verify that supplier/integrator has realistic continuity plans to ensure elements can always be made in time.
e) Verify supplier/integrator has processes that detect significant differences in source materials and ingredients.
f) Verify that integrator has realistic continuity plans to ensure elements can always be made in time.
g) Verify integrator has processes that detect significant differences in elements.
h) Perform/outsource acceptance testing to ensure compliance with performance specifications.
i) Perform evaluations of integrators delivery mechanisms for compliance with processes and procedures implemented to protect the element during production, delivery, and support activities.

3.16: Protect/Monitor/Audit Operational System

The Operational system may consist of a bounded system that is delivered to a given enterprise or it can be defined as an outsourced service delivery system. The nature of the operational environment is to be dynamic and as such, is likely to be subject to vulnerabilities and/or weakness not addressed previously. Contractual requirements should include protecting, monitoring, and auditing the system's elements during operation, while the system is active and at rest, and reporting information such as unauthorized/unexpected activities. Additionally, personnel security requirements, particularly those that emphasize people who implement supply chain processes for systems and elements, including those personnel security controls contained in NIST SP 800-53 and FIPS199 high-impact system specification, should be employed to protect the operational system.

This key practice applies to both the bounded operational system within the acquirers' environment which may require multi tiered-supplier operational support, as well as the outsourced operational systems within the suppliers' environment, remotely used

by the acquirer. The integrator is considered a pre operational service provider within the system life cycle and as such, is not the focus of this key practice.

3.16.1 Acquirer - Programmatic Activities

a) Require that the system's operational environment will protect the system physically and logically. Leverage existing requirements/methods, e.g., NIST SP 800-53.
b) Require continuous monitoring activities on the operational system as outlined in NIST SP 800-37.
c) Include supply chain considerations and requirements in contracts for operational systems and outsourced services.
d) Require, where applicable, periodic independent third-party audits of supplier systems.
e) Include applicable system integration and custom code extension activities as part of the upgrade and maintenance efforts in system operational requirements.
f) Develop and implement an approach for handling and processing reported supply chain anomalies.

3.16.2 Integrator – General Requirements

a) None

3.16.3 Supplier - General Requirements

a) Report supply chain anomalies in operational environments to agreed-upon recipient within established time frame parameters.

3.16.4 Integrator – Technical Implementation Requirements

a) None.

3.16.5 Supplier - Technical Implementation Requirements

a) Protect system's elements from tampering by using a variety of methods such as robust configuration management, limited privileges, checking cryptographic hashes, and applying anti-tamper techniques. Reference guidance provided in the DHS document, *Software Assurance (SwA) in Acquisition: Mitigating Risks to the Enterprise*.
b) Establish a trusted baseline for the system and operations. Use this baseline to identify unauthorized changes or tampering.

c) Use existing vulnerability and incident management capabilities to identify potential supply chain vulnerabilities. Leverage the Security Content Automation Protocol (SCAP) or similar capabilities where possible.

3.16.6 Integrator - Validation and Verification Requirements

a) None

3.16.7 Supplier - Validation and Verification Requirements

a) Use multiple and complementary monitoring/audit approaches and leverage existing data to analyze for supply chain risk.
b) Confirm (manually and/or automatically) that the operational configuration profile is correct. Report findings if actual operations differ from the expected (or baseline) operational profile. Such profiles could consider time of use, information being used (e.g., directories), applications/equipment used, and connections used.

3.16.8 Acquirer - Validation and Verification Requirements

a) Monitor and audit supplier system activities for compliance with requirements and to detect potential supply chain issues, such as the presence of malicious functionality, known vulnerabilities, or changes in suppliers or supplier personnel. This should include applicable system integration and custom code extension activities as part of the upgrade and maintenance efforts for system operations.
b) Monitor and audit systems and operations to reduce the risk of unauthorized element(s) removal, replacement, and/or modification.
c) Determine appropriate recipients of operational reports, and require deployment of reporting systems to ensure timely, accurate, and reliable delivery of such reports. These recipients may include the supplier, the acquirer, or the user.

3.17: Negotiate Requirements Changes

Adding requirements or unconstrained requirement changes can create new or increased supply chain risks. Each additional requirement may add elements, element features, interfaces, or new interdependencies or processes, resulting in additional suppliers or complexity (in systems, elements, and/or processes). Adding additional system or element features typically increases complexity, which in turn creates opportunities for exposure and potential new vulnerabilities.

3.17.1 Acquirer - Programmatic Activities

a) Develop standard language that can be included in contracting provisions defining processes for negotiating changes in requirements to ensure acquisition and procurement activities can continue without having to terminate and restart.
b) Work with stakeholders to prioritize when certain requirements must be incorporated; delay adding features if they can be postponed to the next increment or block.
c) Negotiate requirement changes in a manner that does not unduly limit COTS and GOTS options.

3.17.2 Integrators - General Requirements

a) Include processes for negotiating changes in requirements and acquisition/procurement activities.
b) Negotiate requirements changes in a manner that does not unduly limit COTS or GOTS options.

3.17.3 Suppliers - General Requirements

a) None.

3.17.4 Integrators - Technical Implementation Requirements

a) Identify, for each proposed change in an operational or technical requirement, technical specification, or mandatory business practice: 1) functions to be added, modified, or removed; 2) interfaces to other elements or processes that will be affected; 3) weaknesses or deficits, faults or vulnerabilities, and opportunities for exposure of or access to systems, elements, or processes that will be affected; and 4) suppliers or acquirers who will either enter or exit the supply chain.

3.17.5 Suppliers - Technical Implementation Requirements

a) None

3.17.6 Integrators - Validation and Verification Requirements

a) Assess proposed changes in the supply chain resulting from requirements changes for additional deficits or faults that could create new increased opportunities of adversary exposure of or access to elements, element processes, or supplier business processes.
b) Investigate and propose measures that could be employed to prevent exposure of or access to elements, processes, and suppliers in the event that proposed supply chain changes are adopted.
c) Evaluate changes in the supply chain environment or context of use under which additional protective measures might be required in order to assure or

enhance the current level of confidence in the confidentiality, integrity, and availability of elements.

3.17.7 Suppliers - Validation and Verification Requirements

a) None

3.17.8 Acquirer - Validation and Verification Activities

a) Review and assess negotiated changes in operational and technical requirements, technical specifications, and mandatory mission/business practices, and report assessments results to stakeholders.
b) Review and evaluate the integrators' assessments of changes to system or element features and functions, as well as the addition or deletion of suppliers, and the protective measures selected for implementation associated with each change.
c) Review and assess requirements; remove requirements if possible while still meeting user needs.

3.18: Manage Supply Chain Vulnerabilities

Upon discovery of a supply chain vulnerability, supply chain stakeholders (acquirers, integrators, and suppliers) initiate a vulnerability management process to determine actions or allocate resources to limit the vulnerability's adverse consequences. Supply chain vulnerability management begins when a vulnerability in an element's/system's supply chain is discovered and identified. Then a determination is made as to the potential impact of exploitation and the dependencies across the supply chain whether or not the vulnerability is being exploited, if known, and where the vulnerability was introduced. The level of risk generated by this vulnerability is determined, and a decision is made to mitigate or accept the risk.

3.18.1 Acquirer – Programmatic Activities

a) Require establishment of a process for managing supply chain vulnerabilities, including detecting, tracking/logging, selecting a response, performing the response, and documenting the response.
b) Prioritize activities to focus on critical elements based on the potential for higher severity of consequences.

3.18.2 Integrators – General Requirements

a) Establish a process for managing supply chain vulnerabilities including detecting, tracking/logging, selecting a response, performing the response, and documenting.
b) Prioritize activities to focus on critical elements based on the potential for higher severity of consequences.

3.18.3 Suppliers – General Requirements

a) Establish a process for managing supply chain vulnerabilities including detecting, tracking/logging, selecting a response, performing the response, and documenting the response.

3.18.4 Integrators – Technical Implementation Requirements

a) Implement plan to remediate vulnerabilities upon detection, to identify the weakness associated with the vulnerability, to determine the root cause and context, and to determine the likelihood of its exploitation and the severity of its consequences.
b) Document the vulnerability identified, including the weakness, the root cause and context, the determined likelihood of exploitation and severity of its consequences. Include documentation of resolution when vulnerability is remediated. Work with suppliers, as appropriate, to obtain root cause and resolution.

3.18.5 Suppliers – Technical Implementation Requirements

a) Implement plan to remediate vulnerabilities upon detection, to identify the weakness associated with the vulnerability, determine the root cause and context, and determine the likelihood of its exploitation and the severity of its consequences.

3.18.6 Integrators – Validation and Verification Requirements

a) Monitor and assess supply chain vulnerability analysis and remediation.
b) Monitor suppliers of elements of the same family (e.g., similar commoditized elements) to learn of newly discovered vulnerabilities.
c) Notify acquirer/vendor of newly discovered vulnerabilities.

3.18.7 Suppliers – Validation and Verification Requirements

a) Monitor and assess SCRM vulnerability analysis and remediation across their supply chain for the elements provided.
b) Notify acquirer/integrator of newly discovered vulnerabilities.

3.18.8 Acquirer – Validation and Verification Activities

a) Monitor and assess acquirer SCRM vulnerability analysis and remediation process.
b) Monitor suppliers of elements of the same family (e.g., similar commoditized elements) to learn of newly discovered vulnerabilities.

c) Ensure integrator implements a SCRM vulnerability analysis and remediation process.

3.19: Reduce Supply Chain Risks during Software Updates and Patches

Software updates and patches can change the system in ways that create new vulnerabilities. On the other hand, failing to update software or apply a patch promptly may leave a known vulnerability in place that an adversary could exploit. Supply chain risks should be considered during software updates and patch management.

3.19.1 Acquirer – Programmatic Activities

a) Utilizing the guidance contained in NIST SP 800-40, *Creating a Patch and Vulnerability Management Program*, develop organizational policy and procedures on implementing software updates and patch management. These policies and procedures should provide the conditions under which updates and patches will be evaluated for authenticity and correctness, including the anticipated impact on elements, processes, and uses.

3.19.2 Integrators – General Requirements

a) Implement a formal written procedure on system/element software update and patch management. It should articulate the conditions under which updates and patches will be evaluated for authenticity and correctness, including the anticipated impact on elements, processes, and uses.

3.19.3 Suppliers – General Requirements

a) Implement policies on element software update and patch management. It should articulate the conditions and sources under which updates and patches are delivered or made available to customers.

3.19.4 Integrators – Technical Implementation Requirements

a) For each software element of the system, determine if each update/patch will be evaluated individually, or if the supplier or supplier's patch management process will be evaluated periodically. If the update/patch or the associated patch management process will be evaluated, determine the evaluation criteria and process.
b) For each software element of the system, determine if the supplier and its delivery method meet requirements.
c) Examine significant software patches and upgrades as if they are new elements for trustworthiness, including delivery mechanisms.

d) Authenticate the patch source (e.g., digitally signed patches) to ensure the integrity of the patch.
e) Verify that the patch administrator has the appropriate credentials and access privileges for the role and that their activities are monitored for supply chain impact. For open source elements, ensure that update sources are sanctioned and approved by the integrator.

3.19.5 Suppliers – Technical Implementation Requirements

a) Provide trustworthy patch and update processes including the authentication of the patch and or update source (e.g., digitally signed patches).

3.19.6 Integrators – Validation and Verification Requirements

a) Ensure that patches are signed, are not tampered with during delivery, and are applied to the system in the same state as they were when they were produced.
b) Verify that the delivery mechanism is as defined, e.g., strength of authentication and encryption mechanism.
c) Verify that the updated system works as intended with patches and/or updates installed.
d) Verify authenticity of patches including non scheduled or out-of-sequence patching.
e) Verify updates and patches against the system to be delivered to ensure updates/patches have not "broken" anything that was working.

3.19.7 Suppliers – Validation and Verification Requirements

a) Verify that each patch is digitally signed before it available to customers.

3.19.8 Acquirer – Validation and Verification

a) Verify digital signatures to ensure patches are not tampered with during delivery and are applied to the system in the same state as they were when they were produced.
b) Verify that delivery mechanism is as defined, e.g., strength of authentication and encryption mechanism.
c) Verify authenticity of patches including non scheduled or out-of-sequence patches.

3.20: Respond to Supply Chain Incidents

A supply chain incident occurs when an element has been exposed or exploited resulting in a loss of confidentiality, integrity, or availability. Organizations should plan and establish a process for managing supply chain incidents, including detecting and reporting incidents, and then selecting and implementing a response. For more

information, see NIST SP 800-100, Information Security Handbook: A Guide for Managers; NIST SP 800-61, Revision 1, Computer Security Incident Handling Guide; NIST SP 800-83, Guide to Malware Incident Prevention and Handling; and NIST SP 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, Operational Family: Incident Response.

3.20.1 Acquirer – Programmatic Activities

a) Define the context and events, activities, or behaviors that would constitute a supply chain "incident" for specific elements, processes, or systems. Additionally define scope incident occurrence process, classification of incident types, and appropriate response.
b) Define supply chain incident attributes to be recorded in an appropriate manner, such as the element or process displaying or demonstrating anomalous behavior or the discovery of a counterfeit element, the time and place of the anomalous behavior or discovery, the method or mechanism by which the incident was detected, and the suspected or known identity or source of the incident.
c) Collaborate with the integrator when incidents occur to ensure appropriate resolution for both parties.
d) Coordinate supply chain incident management activities with other organizations to ensure consistent and effective management of supply chain incidents, such as establishing and maintaining supply chain incident reporting connectivity to local, regional, and national incident management processes where established (e.g., IAVA, CERT/CC, US CERT, FBI) and possibly intelligence processes. Follow established procedures for reporting incidents.

3.20.2 Integrators – General Requirements

a) Define and assign specific roles and responsibilities for managing and reporting SCRM incidents including the collection, processing, and dissemination of SCRM incident information, the timeline and method for SCRM information reporting, and the distribution of SCRM information.
b) Develop and implement processes required to detect SCRM incidents (see the other key practices).
c) Develop and implement formats and/or forms for the reporting of SCRM incidents.
d) Collaborate with the acquirer when incidents occur to ensure appropriate resolution for both parties.
e) Exercise, test, and implement supply chain incident management plans.
f) Establish and maintain a protected and access-controlled supply chain risk incident repository.
g) Coordinate supply chain incident management activities with other organizations to ensure consistent and effective management of supply chain

incidents, such as establishing and maintaining supply chain incident reporting connectivity to local, regional, and national incident management processes where established (e.g., IAVA, CERT/CC, US CERT, FBI, FISMA reporting) and possibly intelligence processes. Follow established procedures for reporting incidents.

3.20.3 Suppliers – General Requirements

a) Exercise, test, and implement supply chain incident management plans.
b) Establish and maintain a protected and access-controlled supply chain risk incident report repository.
c) Establish consistent and effective processes for the management of supply chain incidents, such as maintaining an supply chain incident reporting connection to local, regional, and national incident management processes where established (e.g., CERT/CC, US CERT) and formalized procedures for reporting incidents.

3.20.4 Integrators – Technical Implementation Requirements

a) Perform failure or forensic analysis on elements and processes to determine the cause of failure. Isolate and diagnose the elements of the component that are not performing properly and assess the origin and mechanisms of the failure. Assess the impact of the failure, ways to detect failures, and mitigating actions (including ways to detect failures and preventing future occurrences).
b) Document and report the incident and all related findings, per contractual agreement.

3.20.5 Suppliers – Technical Implementation Requirements

a) Perform failure or forensic analysis on elements and processes to determine the cause of failure. Isolate and diagnose the elements of the component that are not performing properly and assess the origin and mechanisms of the failure. Assess the impact of the failure, ways to detect failures, and mitigating actions (including ways to detect failures and prevent future occurrences).
b) Document and report the incident and all related findings.

3.20.6 Integrators – Validation and Verification Requirements

a) Perform trend analysis on supply chain incident statistics (including who performs, and who receives results).

3.20.7 Suppliers – Validation and Verification Requirements

a) Perform trend analysis on supply chain incident statistics (review who performs the analysis, and who receives results).

3.20.8 Acquirer – Validation and Verification Activities

a) Verify that the suppliers/integrators have a protected and access-controlled supply chain risk incident report repository.
b) Perform trend analysis on supply chain incident statistics (including who performs, and who receives results).

3.21: Reduce Supply Chain Risks During Disposal

Poor disposal procedures can lead to unauthorized access to systems/elements. There are often new actors in disposal processes who are not aware of supply chain threats or procedures. NIST SP 800-88, *Guidelines for Media Sanitization*, assists organizations in implementing a media sanitization program with proper and applicable techniques and controls for sanitization and disposal decisions. This practice builds on the guidance provided in that document.

3.21.1 Acquirer - Programmatic Activities

a) Ensure disposal requirements are included in procurement documents.
b) Negotiate and define disposal practices with suppliers/integrators to align planning and procedures during the system and associated elements' lifetime, including authorized service personnel's access to authentic parts and the handling of damaged or retired elements, a listing of parts, and the data retention (if any) capability of each.
c) Develop organization policy and procedures that :
    a. Require that any counterfeit parts detected will be seized, destroyed, or preserved for law enforcement evidentiary purposes (not returned to the source/supply chain); otherwise, such items may be used to develop future counterfeit/subverted elements. The counterfeit and subverted elements should be shared with the authentic supplier for forensic analysis. If there is no forensic or evidentiary value, then counterfeit parts should be destroyed by reputable disposers that have been validated by authentic original suppliers or trained law enforcement authorities.
    b. Encourage the selection of elements that can be disposed in a way that does not expose protected information, for example, elements that permit offloading of data prior to disposal or elements that are easy to wipe clean prior to disposal.

    c. Require use of trusted disposers, as appropriate (in some cases, they may need to be cleared).
    d. Require procedures for the secure and permanent destruction of elements, as appropriate.

d) When required for forensic investigation or for later comparison for detection of counterfeits, surrender elements for disposal to a dedicated repository.
e) Establish the end-of-life support process for systems/elements.

3.21.2 Integrators - General Requirements

a) Train all personnel involved in the disposal process on supply chain risk and internal procedures.
b) Encourage the selection of elements that can be disposed of in a way that does not expose protected information, for example, elements that permit offloading of data prior to disposal, or elements that are easy to wipe clean prior to disposal.
c) Business practices should prohibit transmission or distribution of acquirer's sensitive data or sensitive elements to unauthorized or unspecified parties during disposal activities.
d) When required for forensic investigation or for later comparison for detection of counterfeits, surrender elements for disposal to a dedicated repository.
e) Require use of trusted disposers, as appropriate (in some cases, they may need to be cleared).
f) Implement procedures for the secure and permanent destruction of elements.
g) Engage trained disposal service personnel and set expectations for the procedures that conform to the acquirer's disposal policy.

3.21.3 Suppliers - General Requirements

a) Establish relationship with trusted disposers who have demonstrated an effective disposal process
b) Implement processes and procedures for the secure and permanent destruction of elements, as appropriate.

3.21.4 Integrators – Technical Implementation Requirements

a) Ensure that scrap materials, out-of-specification elements, or suspect or confirmed defective, counterfeit, or tampered components are controlled, preserved for appropriate evidentiary or forensic purposes, and disposed of properly.
b) Identify all elements/sub-elements that need to be specially disposed of (including HAZMAT/explosive ordinance/environment impact, confidential equipment, etc.).

c) Carefully move, save, remove, and/or destroy data so that it does not harm, lose, or corrupt required information and does not expose acquirer's sensitive information.
d) Maintain a system to inventory and record disposal of controlled items.
e) Describe the organizational disposal capabilities for elements/systems in support of the acquirer's policy either in an RFI response or in general program support documentation.

3.21.5 Suppliers - Technical Implementation Requirements

a) Manage and properly dispose of all scrap materials, out-of-specification elements, or suspect or confirmed defective, counterfeit, or tampered components.
b) Establish process used to identify all elements/sub-elements that need to be specially disposed of (including HAZMAT/explosive ordinance/environment impact, confidential equipment, etc.).
c) Document the process used to carefully move or save data so that it does not harm, lose, or corrupt required information and does not expose acquirer's sensitive information.
d) Describe technical limitations related to disposal activities (e.g., degaussed media cannot be reused and will void warranties).

3.21.6 Integrators - Validation and Verification Requirements

a) Ensure the adequacy of the destruction method for controlled items.
b) Verify supplier's security procedures to govern the transfer of elements and acquirer's sensitive information.
c) Ensure that items subject to controlled disposal are accurately identified, marked, and recorded for traceability.

3.21.7 Suppliers - Validation and Verification Requirements

a) Regularly review the disposal process.
b) Verify and validate the identification and tracking of items subject to preservation for forensics and evidentiary purposes and/or controlled disposal.

3.21.8 Acquirer - Validation and Verification Activities

a) Assess integrators' and suppliers' capability to meet the disposal requirements including the capacity of non disk drive elements (e.g., memory boards) to retain data under certain conditions.
b) Periodically review the acquirer's organizational disposal process.
c) Ensure the adequacy of the destruction method for controlled items.

d) Ensure that supplier/integrator's disposal procedures meet specified requirements.

APPENDIX A GLOSSARY

Access	Ability to make use of any information system (IS) resource.
Acquirer	For this document, the acquirer is always a government agency (including those agencies taking on the role of integrator).
Agreement Processes [ISO/IEC 15288:2008]	Produce negotiated terms and conditions by which organizations obtain or provide products/services to other entities, including contracts, grants, cooperative agreements, and other transactions.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Component	Synonym for element.
Critical Component	A system element that, if compromised or failed, could cause mission or business failure or compromise security.
Defense-in-Breadth – [CNSSI-4009]	A planned, systematic set of multi disciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).
Defense-in-Depth – [CNSSI-4009; SP 800-53]	Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.
Degradation	The decline in the quality or performance of what is being sampled; the process by which declining the quality or performance is brought about.
Element	Includes: COTS and GOTS (software, hardware and firmware) and synonymous with components, devices, products, systems, and materials. A part of a system. Synonym for component. An element may be implemented by products or services.
Element Processes	A series of operations performed in the making or treatment of an element; performing operations on elements/data.
Identity	The set of physical and behavioral characteristics by which an individual is uniquely recognizable. The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.
Industrial Security	The portion of internal security which refers to the protection of industrial installations, resources, utilities, materials, and classified information essential to protect from loss or damage.

Information Assurance (IA) [CNSSI No. 4009]	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
Integrator	For this document, it is always a third-party organization that specializes in combining products/elements of several suppliers to produce elements (information systems).
Life cycle	A progression through a series of differing stages of development. Commonly referred to as system development life cycle (SDLC). The course of events that brings a new product into existence and follows its growth into a mature product and into eventual critical mass and decline.
Manufacturer	A person or business that makes or builds something.
Mitigation	An action taken to reduce or eliminate a risk.
Monitoring Procedures	A set of instructions that observes, supervises, or controls the activities of other programs.
Network	A complex, interconnected group or system.
Patch	An update to an operating system, application, or other software issued specifically to correct particular problems with the software.
"Red Team" Approach	A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.
Risk [CNSSI No. 4009] [NIST Special Pub 800-53 Rev 3: FIPS 200, adapted]	A possibility that a particular threat will adversely impact an IS by exploiting a particular vulnerability. 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. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Risk Analysis [CNSSI No. 4009]	Examination of information to identify the risk to an IS risk assessment. Process of analyzing threats to and vulnerabilities of an IS, and the potential impact resulting from the loss of information or capabilities of a system. This analysis is used as a basis for identifying appropriate and cost-effective security countermeasures.

Risk Management (RM) [NIST Special Pub 800-53 (Rev 2)] [CNSSI No. 4009]	Process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.
[NIST Special Pub 800-53, Rev 3]	The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
Secure by Default	Initial or default configuration involving disabling as many attackable services as possible while still leaving a useful system.
Supplier	Third-party organization providing individual elements.
Supply Chain [Engineering for System Assurance, National Defense Industry Association (NDIA), Sep 2008]	The set of organizations, people, activities, information, and resources for creating and moving a product or service (including its sub-elements) from suppliers through to an organization's customers.
Supply Chain Assurance	Confidence that the supply chain will produce and deliver elements, processes, and information that perform as required.
Susceptibility [DoDI 3020.45]	The inherent capacity of an asset to be affected by one or more threats or hazards.
Susceptibility Analysis	Examination of all susceptibility information to identify the full range of mitigations desired or possible that will diminish the impacts from exposure of vulnerabilities or access by threats.
Susceptibility Assessment	Formal description and evaluation of susceptibilities sufficient for decision makers to select one or multiple risk managing actions, such as accept, mitigate, transfer, or indemnify.
System [ISO/IEC 15288:2008]	A combination of interacting elements organized to achieve one or more stated purposes.
System Assurance [NDIA 2008]	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 Life cycle	The phases of a system or proposed system that address its existence from inception to retirement.
Threat [CNSSI No. 4009]	Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Threat Analysis [CNSSI No. 4009]	Examination of information to identify the elements comprising a threat.
Threat Assessment [CNSSI No. 4009]	Formal description and evaluation of threat to an IS.
Transparency	Implies openness, communication, and accountability.
Trust [Software Assurance in Acquisition: Mitigating Risks to the Enterprise, NDU, October 22, 2008,]	The confidence one element has in another, that the second element will behave as expected.
Trustworthiness [Software Security Assurance: A State of the Art Report (SOAR), Information Assurance Technology Analysis Center (IATAC) and Defense Technical Information Center (DTIC), July 2007.]	Justifiable confidence that the system/element will perform correctly, which includes predictably behaving in conformance with all of its required critical properties.
Update (a Certificate) [SP 800-32; CNSSI-4009]	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Verifying Procedures	A set of instructions to determine or test the truth or accuracy of, as by comparison, investigation, or reference.
Visibility	The capability of being easily observed.
Vulnerability [CNSSI No. 4009]	Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited.
Vulnerability Analysis [CNSSI No. 4009]	Examination of information to identify the elements comprising a vulnerability.
Vulnerability Assessment [CNSSI No. 4009]	Formal description and evaluation of vulnerabilities of an IS.

APPENDIX B ACRONYMS

ANSI –	American National Standards Institute
AO –	Authorizing Official
API –	Application Programming Interface
BINCS –	Business Identification Number Cross-Reference System
CAGE –	Commercial and Government Entity
CCR –	Central Contractor Registry
CERT/CC –	CERT Coordination Center
CIO –	Chief Information Officer
CISO –	Chief Information Security Officer
CM –	Configuration Management
CNCI –	Comprehensive National Cybersecurity Initiative
CNSS –	Committee on National Security Systems
CO –	Contracting Officer
COOP –	Continuity of Operations
COTS –	Commercial Off-The-Shelf
COTR –	Contracting Officer's Technical Representative
CPI –	Critical Program Information
CPIC –	Capital Planning and Investment Control
CRADA –	Cooperative Research and Development Agreement
CWE –	Common Weakness Enumeration
DHS –	Department of Homeland Security
DIA –	Defense Intelligence Agency
DISA –	Defense Information Systems Agency
DoD –	Department of Defense
DUNS –	Dun and Bradstreet

FAR –	Federal Acquisition Regulation
FBI –	Federal Bureau of Investigation
FDCC –	Federal Desktop Core Configuration
FIPS –	Federal Information Processing Standards
FISMA –	Federal Information Security Management Act
GCC –	GNU Compiler Collection
GIG –	Global Information Grid
GITWG –	Global Information Technology Working Group
GOTS –	Government Off-The-Shelf
GSA –	General Services Administration
GSSP –	GIAC Secure Software Programmer (Certification)
HAZMAT –	Hazardous Materials
IA –	Information Assurance
IAVA –	Information Assurance Vulnerability Alert
IC –	Intelligence Community
ICT –	Information and Communication Technology
IEC –	International Electrotechnical Commission
IP –	Internet Protocol
IS –	Information System
ISO –	International Organization of Standardization
ISSO –	Information Systems Security Officer
IT –	Information Technology
ITL –	Information Technology Laboratory (NIST)
ITSCC –	IT Sector Coordinating Council
JIT –	Just in Time
MTFB –	Mean-time-between-failures
NASPO –	North American Security Products Organization

NDIA–	National Defense Industrial Association
NIST –	National Institute of Standards & Technology
NSA –	National Security Agency
OEM –	Original Equipment Manufacturer
OMB –	Office of Management and Budget
OWASP –	Open Web Application Security Project
PMO –	Program Management Office
R&D –	Research and Development
RFI –	Request for Information
RFP –	Request for Proposal
RFQ –	Request for Quote
RM –	Risk Management
SAISO –	Senior Agency Information Security Officer
SANS –	SysAdmin, Audit, Network, Security (Institute)
SC –	Supply Chain
SCAP –	Security Content Automation Protocol
SCRM –	Supply Chain Risk Management
SCRMC –	Supply Chain Risk Management Capability
SDLC –	System Development Life cycle
SE –	System Engineer
SIC –	Standard Industrial Classification
SLA –	Service-Level Agreement
SOP –	Standard Operating Procedure
SOW –	Statement of Work
STIG –	Security Technical Implementation Guides
SW –	Software
SwA –	Software Assurance

T&E –	Test and Evaluation
TAC –	Threat Assessment Center
TEP –	Technical Evaluation Panel
US –	United States (of America)
US-CERT –	United States Computer Emergency Readiness Team
USA –	United States Army

APPENDIX C REFERENCES

The Common Criteria Evaluation and Validation Scheme, *Home Page 2008,* URL: http://www.niap-ccevs.org/cc-scheme/, accessed 12-18-2008.

Department of Treasury, Office of Investment Security, Guidance Concerning the National Security Review Conducted by the Committee on Foreign Investment in the United States. Guidance, 2007, URL: http:/www.treasury.gov/offices/international-affairs.cfius/docs/GuidanceFinal_12012008.pdf, accessed 12-18-2008.

Committee on National Security Systems Instruction 4009, *National Information Assurance (IA) Glossary,* Revised June 2006, URL: http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf, accessed 12-18-2008.

Data and Analysis Center for Software (DACS), *Software Development Security: A Risk Management Perspective*. DoD Software Tech News. July 2005.

Department of Defense, Defense Information Systems Agency, Information Assurance Support Environment, *Security Technical Implementation Guides Index Page,* URL: http://iase.disa.mil/stigs/stig/index.html, accessed 12-18-2008.

DISA Application Security Project, Developer's Guide to Secure Use of Software Components. Draft Ver. 3.0, October 2004.

DHS National Cyber Security Division *Security in the SW Lifecycle: Making Software Processes and the SW Produced by Them – More Secure, Section 3.5 and Appendix G: G.5.* Draft Version 2.1, August 2006 and Defense Information Systems Agency, *Application Security Project, Developer's Guide to Secure Use of Software Components.* Draft Ver. 3.0, October 2004.

Global Information Technology Working Group (GITWG) of the Committee on National Security Systems (CNSS), Framework for Lifecycle Risk Mitigation for National Security Systems in the Era of Globalization: A Defense-in-Breadth Approach, CNSS Report CNSS-145-06, November 2006.

Goertzel, Karen, et al., Software Security Assurance: A State of the Art Report (SOAR), Information Assurance Technology Analysis Center (IATAC) and Defense Technical Information Center (DTIC), July 2007.

Howard & Lipner, 2007, chapters 9, 21. The Security Development Lifecycle, Microsoft Press.

Information Assurance Technology Analysis Center (IATAC), Data and Analysis Center for Software (DACS). Software Security Assurance: State-of-the-Art Report, Section 5.2.3.1, "Threat, Attack, and Vulnerability Modeling and Assessment."

International Organization for Standardization, *Systems and Software Engineering – System Life Cycle Processes,* 2008, URL: http://www.iso.org/iso/catalogue_detail?csnumber=43562, accessed 12-18-2008.

National Defense Industry Association (NDIA), *Engineering for System Assurance,* September 2008, version 1.0, aka *NDIA System Assurance Guidebook,* http://www.acq.osd.mil/sse/ssa/docs/SA-Guidebook-v1-Oct 2008.pdf, accessed 12-18-2008.

National Defense University (NDU), *Software Assurance in Acquisition: Mitigating Risks to the Enterprise,* October 2008, URL: https://buildsecurityin.us-cert.gov/swa/downloads/SwA_in_Acquisition_102208.pdf, accessed 12-18-2008.

National Institute of Standards and Technology, Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules,* May 2001.

National Institute of Standards and Technology, Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems,* February 2004.

National Institute of Standards and Technology, Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006.

National Institute of Standards and Technology, Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*: *A Security Life Cycle Approach*, February 2010.

National Institute of Standards and Technology, Special Publication 800-40, Revision 2, *Creating a Patch and Vulnerability Management Program*, November 2005.

National Institute of Standards and Technology, Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program,* October 2003.

National Institute of Standards and Technology, Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems,* August 2009.

National Institute of Standards and Technology, Special Publication 800-61, Revision 1, *Computer Security Incident Handling Guide*, March 2008.

National Institute of Standards and Technology, Special Publication 800-70 Revision 1, *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*, September 2008.

National Institute of Standards and Technology, Special Publication 800-88, *Guidelines for Media Sanitization*, September 2006.

National Institute of Standards and Technology, Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.

National Institute of Standards and Technology, Draft Special Publication 800-128, *Guide for Security Configuration Management of Information Systems*, March 2010.

Open Web Application Security Project (OWASP) Top 10 Project, 2007, URL: http://www.owasp.org/index.php/Top_10_2007

OSSTMM – Open Source Security Testing Methodology Manual, http://www.isecom.org/osstmm/

A Guide to the Project Management Book of Knowledge, 2004, 3d ed. Washington DC Project Management Institute.

SafeCode, *Fundamental Practices for Secure Software Development*, October 8, 2008, URL, http://www.safecode.org/publications/SAFECode_Dev_Practices1108.pdf, accessed 2008-12-18.