

The attached DRAFT document (provided here for HISTORICAL purposes) has been superseded by the following publication: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

# Draft NISTIR 7622

---

## Notional Supply Chain Risk Management Practices for Federal Information Systems

Jon Boyens  
Celia Paulsen  
Nadya Bartol  
Rama Moorthy  
Stephanie Shankles

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

DRAFT

**Draft NISTIR 7622**

# Notional Supply Chain Risk Management for Federal Information Systems

Jon M. Boyens  
*Computer Security Division  
Information Technology Laboratory  
National Institute of Standards and Technology  
Gaithersburg, MD 20899*

Celia Paulsen  
*Computer Security Division  
Information Technology Laboratory  
National Institute of Standards and Technology  
Gaithersburg, MD 20899*

Nadya Bartol  
*Booz Allen Hamilton*

Rama S. Moorthy  
*Hatha Systems*

Stephanie A. Shankles  
*Booz Allen Hamilton*

March 2012



**U.S. Department of Commerce**  
*John E. Bryson, Secretary*

**National Institute of Standards and Technology**  
*Patrick D. Gallagher, Under Secretary for  
Standards and Technology and Director*

# DRAFT

## Acknowledgments

The authors, Jon Boyens, National Institute of Standards and Technology (NIST), Celia Paulsen (NIST) Rama Moorthy (Hatha Systems), and Nadya Bartol and Stephanie Shankles (Booz Allen and Hamilton), would like to acknowledge and thank Marianne Swanson, NIST, for her leadership in initiating this project as well as in the development of the document's initial public draft. We would like to thank Dan Reddy (EMC), Edna Conway (Cisco), and Hart Rossman (SAIC) for their comments and suggestions.

We would also like to thank the members of the Comprehensive National Cybersecurity Initiative (CNCI) 11 Lifecycle Processes and Standards Working Group and their support contractors as well as members of the Information Technology (IT) 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. Additionally, we would like to thank Dr. Sandor Boyson and the University of Maryland's Supply Chain Management Center for their research on ICT SCRM, which provided valuable contributions for this document.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

## DRAFT

### Note to Reviewers

This Draft NIST Interagency Report (NISTIR) 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 (SPs) like NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*; the National Defense University, *Software Assurance in Acquisition: Mitigating Risks to the Enterprise*; and the National Defense Industrial Association (NDIA), *Engineering for System Assurance*, and then expanded upon to include supply chain-specific implications. Additional guidance that may have supply chain implications includes, but is not limited to, International Traffic in Arms Regulations (ITAR) and Customs-Trade Partnership Against Terrorism (CTPAT).

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.

NIST is looking for public feedback on how to differentiate more and less critical components in addition to the information described in Draft NIST SP 800-53 Revision 4 SA-14 and SA-15.

NIST is also seeking threat models or other relevant information for use in developing an ICT supply chain risk assessment matrix and threat scenarios.

Additionally, NIST is looking for feedback regarding what information that is being described in this document is already collected in response to other legislation, regulations, and standards.

Comments on the document should be sent to: [scrm-nist@nist.gov](mailto:scrm-nist@nist.gov) by May 11, 2012. Comments and lessons learned on using the practices should be sent to the same e-mail address on an ongoing basis.

**Table of Contents**

<b>Acknowledgments</b>	_____	<b>iii</b>
<b>Note to Reviewers</b>	_____	<b>iii</b>
<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Purpose	2
1.2	Scope	2
1.3	Background (history and industry collaboration)	3
1.4	Key Definitions	3
1.5	Related Documents	4
1.6	Document Structure	5
<b>2</b>	<b>Overview</b>	<b>6</b>
2.1	Challenges	6
2.2	Success Factors	7
<b>3</b>	<b>Implementing Supply Chain Risk Management</b>	<b>9</b>
3.1	Roles and Responsibilities for Information and Communication Technology Supply Chain Risk Management	9
3.2	Information and Communication Technology Supply Chain Risk Management Implementation Process	11
<b>4</b>	<b>Supply Chain Risk Management Practices</b>	<b>22</b>
4.1	Uniquely Identify Supply Chain Elements, Processes, and Actors	24
4.2	Limit Access and Exposure within the Supply Chain	28
4.3	Create and Maintain the Provenance of Elements, Processes, Tools, and Data	32
4.4	Share Information within Strict Limits	36
4.5	Perform Supply Chain Risk Management Awareness and Training	43
4.6	Use Defensive Design for Systems, Elements, and Processes	46
4.7	Perform Continuous Integrator Review	56
4.8	Strengthen Delivery Mechanisms	60
4.9	Assure Sustainment Activities and Processes	63
4.10	Manage Disposal and Final Disposition Activities Throughout the System or Element Life Cycle	69
<b>APPENDIX A</b>	<b>GLOSSARY</b>	<b>73</b>
<b>APPENDIX B</b>	<b>ACRONYMS</b>	<b>79</b>

<b>APPENDIX C REFERENCES</b>	<b>82</b>
<b>APPENDIX D UMD ICT SUPPLY CHAIN STUDY</b>	<b>85</b>

DRAFT

# 1 Introduction

Federal agency information systems<sup>1</sup> are increasingly at risk of both intentional and unintentional supply chain compromise due to the growing sophistication of information and communications technologies (ICT) and the growing speed and scale of a complex, distributed global supply chain. Federal departments and agencies currently have neither a consistent nor comprehensive way of understanding the often opaque processes and practices used to create and deliver hardware and software products and services that are contracted out, especially beyond the prime contractor. This lack of understanding, visibility, and control increases the risk of exploitation through a variety of means including counterfeit materials, malicious software, or untrustworthy products, and makes it increasingly difficult for federal departments and agencies to understand their exposure and manage the associated supply chain risks. Currently, federal departments and agencies and private sector integrators and suppliers use varied and nonstandard practices.

The ICT supply chain is a globally distributed, interconnected set of organizations, people, processes, services, products, and other elements. It extends across the full system development life cycle including research and development (R&D), design/development, acquisition of custom or commercial off-the-shelf (COTS) products, delivery, integration, operations, and disposal/retirement.

A multi-pronged approach is the best way to build assurance into the systems and components that the federal government procures and manages. Such an approach may include: Federal Acquisition Regulations (FAR) that require supply chain practices; widely adopted or international standards on supply chain practices for integrators and suppliers; a means to share supplier-related threat information; current and new technologies and tools incorporated into supply chain practices; and increased ability of federal departments and agencies to manage supply chain risks once an information system is in place.

This document seeks to equip federal departments and agencies with a notional set of repeatable and commercially reasonable supply chain assurance methods and practices that offer a means to obtain an understanding of, and visibility throughout, the supply chain. This understanding and visibility will give federal departments and agencies the ability to strategically manage the associated Information and Communication Technology (ICT) supply chain risks over the entire life cycle of products, systems, and services.

Many of the supply chain risk management (SCRM) activities described in this document build on existing business practices to specifically help manage supply chain risks in the evolving threat environment. They originate from within

---

<sup>1</sup> An information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. In the context of this publication, the definition includes the environment in which the information system operates (i.e., people, processes, technologies, facilities, and cyberspace). (NIST SP 800-30)

organizations that already address a variety of business or engineering processes of many disciplines including logistics, reliability, security, and safety. Since ICT SCRM is an enterprise process, leveraging existing knowledge collected for other disciplines enables the development of a commercially reasonable set of activities required to achieve supply chain assurance.

Organizations should select and tailor the practices in this document based on the suitability for a specific application or acquisition and combined impact on the performance, cost, and schedule.

## 1.1 Purpose

This document provides a set of ICT SCRM practices to help federal departments and agencies manage acquisition and implementation of ICT products and services. The SCRM practices are intended to promote a greater understanding of processes and practices used to create and deliver hardware and software that comprise federal information systems. These practices are recommended to be used for those information systems categorized at the Federal Information Processing Standards (FIPS) 199 high-impact level,<sup>2</sup> but in some cases may be applied to moderate- or low-impact level systems.

The practices contained in this document are built on existing practices and are intended to increase the ability of federal departments and agencies to strategically manage the associated ICT supply chain risks over the entire life cycle of products, systems, and services. The practices addressed in this document can be applied to the research and development (R&D), design/development, acquisition of custom or commercial off-the-shelf (COTS) products, delivery, integration, operations, and disposal/retirement activities.

This document does not provide specific contract language, a detailed threat assessment, or a complete list of supply chain assurance methods and techniques that mitigate specific supply chain threats. It is our intent that public and private sector organizations apply these practices and provide NIST with comments on the practicality, feasibility, cost, challenges, and successes of the guidance. NIST intends to expand this document into a NIST Special Publication after additional research is done.

## 1.2 Scope

This document applies to all federal departments and agencies that acquire ICT products and services. It is intended to serve a diverse federal audience including mission/business owners, information system owners, acquisition staff, information

---

<sup>2</sup> 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.

system security personnel, and system engineers responsible for delivering information systems with supply chain assurance.

This document provides guidance for federal agency acquirers on developing acquisitions requirements and potential ways of monitoring whether and how well requirements are implemented. Third-party suppliers and integrators will also find this document useful for insight and understanding of the potential federal operating environment. It also provides guidance for the integrators regarding the expectations they should have for their ICT suppliers.

### **1.3 Background (history and industry collaboration)**

The President's Comprehensive National Cyber Security Initiative (CNCI) 11 is co-chaired by the Department of Defense (DoD) and the DHS. The initiative seeks to provide federal departments and agencies with a 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. Through the work of CNCI 11, an interagency group evaluated a number of source documents and developed an initial set of supply chain assurance methods/techniques or practices that cover the system development life cycle (SDLC) as part of a government wide SCRM solution. The initial public draft of this document was developed using these practices as a foundation. NIST SP 800-53 Rev. 4, *Recommended Security Controls for Federal Information Systems and Organizations*, and *The 25 Point Implementation Plan to Reform Federal Information Technology Management* from the U.S Chief Information Officer (CIO) are also foundational to the development of this document. This draft takes into consideration stakeholder comments and attempts to address many of the recommendations received while maintaining the overall purpose of the document.

### **1.4 Key Definitions<sup>3</sup>**

The following are key terms that will be used throughout this paper. A more complete list of terms is included in Appendix A.

- Acquirer [Source: ISO/IEC 15288, adapted]
  - Stakeholder that acquires or procures a product or service.
- Element
  - Commercial off-the-shelf (COTS) or government off-the-shelf (GOTS) software, hardware, or firmware. Synonymous with components, devices, products, systems, and materials.
- ICT [Source: ANSDIT, adapted]
  - Encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information.
- ICT Supply Chain [Source: ISO 28001, adapted]
  - Linked set of resources and processes between acquirers, integrators, and suppliers that begins with the sourcing of ICT products and services and

---

<sup>3</sup> A complete list of relevant terms and definitions can be found in Appendix A.

- extends through the manufacturing, processing, design, development, handling, and delivery of ICT products and services to the acquirer.
- ICT Supply Chain Risk [Source: NIST Special Pub 800-53 Rev 3: FIPS 200, adapted]
    - 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.
  - Integrator
    - An organization that customizes (e.g., combines, adds, optimizes) elements, processes, and systems. The integrator function can be performed by acquirer, integrator, or supplier organizations.
  - Risk Management [Source: SP 800-53; SP 800-53A; SP 800-37]
    - 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.
  - Supplier [Source: ISO/IEC 15288, adapted]
    - Organization or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain.

## 1.5 Related Documents

United States (U.S.) law and associated policy require federal departments and agencies to use international, voluntary consensus standards in their procurement and regulatory activities, except where inconsistent with law or otherwise impractical.<sup>4</sup> The ICT SCRM approach and key practices (KP) described in this document are rooted in many international standards as well as government and industry documents, which include:

- ISO/IEC 15288: 2088 Systems and software engineering – System life cycle processes;
- NDIA System Assurance Guidebook v1.0;
- *The Software Supply Chain Integrity Framework* (July 21, 2009) and *Software Integrity Controls* (June, 14, 2010) from SAFECODE;
- *Open Trusted Technology Provider Framework (O-TTPF)* A White Paper by: The Open Group Trusted Technology Forum, Feb. 2011;
- Draft ISO/IEC 27036 *Information technology: Security techniques- Information Security for Supplier Relationships*;
- *ISA Guidelines for Securing the Electronics Supply Chain (Draft)*, Internet Security Alliance;
- *Assessing SCRM Capabilities and Perspectives of the IT Vendor Community: Toward a Cyber-Supply Chain Code of Practice*. A NIST-sponsored project

---

<sup>4</sup> “National Technology Transfer and Advancement Act,” “Office of Management and Budget (OMB) Circular A-119 Revised: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities,” and, Trade Agreements Act of 1979, as amended.

conducted by The Supply Chain Management Center Robert H. Smith School of Business, University of Maryland;

- *Recommended Security Controls for Federal Information Systems and Organizations*, NIST SP 800-53 Revision 3 or later; and
- *ICT Supply Chain Threats: Frame of Reference Document*, DHS.

## 1.6 Document Structure

The remainder of the document is organized as follows:

- Section 2, Overview, provides a high-level discussion of ICT supply chain challenges, success factors, and foundational practices.
- Section 3, Implementing SCRM, provides information on how ICT SCRM considerations can be integrated into the federal acquisition life cycle.
- Section 4 provides the ten key practices identified for SCRM throughout the system or element life cycle with specific activities tailored for suppliers, acquires, and integrators. Activities are categorized as Programmatic Activities, General Requirements, Technical Implementation Requirements, and Validation and Verification Activities.
- Appendices

DRAFT

## 2 Overview

This section provides an overview of challenges associated with addressing ICT SCRM and builds the foundation for implementing ICT SCRM practices within individual agencies' enterprise processes. The section sets the stage for the remainder of the document, providing guidance on integrating ICT SCRM into agency enterprise processes and specific ICT SCRM practices.

### 2.1 Challenges

The federal government's reliance on COTS hardware and software is driven by the need for cost reduction, achieving operational efficiencies, and economies of scale. Incorporating COTS hardware and software permits the federal government to leverage the pace of COTS innovation without bearing the development costs of such innovation. While the benefits are substantial, there are also consequences of such reliance that affect the federal government's ability to protect information and information systems.

The growing sophistication of today's ICT, facilitated by the speed and scale of globalization, has given rise to an increasingly complex global ICT supply chain, with logically long and geographically diverse routes, including multiple tiers of outsourcing. This leads to a significant increase in the number of individuals and organizations who "touch" a product, and may allow malicious actors (individual, organization, or nation-state), direct or indirect, to affect the management or operations of companies within their specific territorial jurisdiction that may result in risk to the information system, organization, or Nation. However, global aspects of the supply chain alone are no reason to employ special supply chain risk mitigation practices, as risks must be evaluated in their entirety; even solely domestically developed information system elements contain intentional and unintentional vulnerabilities that may present opportunities for supply chain-related compromises.

Additionally, today's multifaceted global economy and manufacturing practices make corporate ownership and control more ambiguous when assessing supply chain vulnerabilities. For example, foreign-based companies sometimes manufacture and assemble products and components in the United States, and U.S.-based companies sometimes manufacture products and components overseas, or domestically employ foreign workers.

Though globalization and its consequences are permanent and likely to have a greater impact over time, this growing complexity reduces both the depth and breadth of visibility and traceability achievable by the federal acquirer. This lack of visibility and traceability increases the acquirer's risk of not being able to detect and remediate intentional and unintentional compromise which may be introduced through a variety of means, including counterfeit materials or malicious software.<sup>5</sup>

---

<sup>5</sup> For the purposes of this document, products and product components are referred to as "elements."

Currently, federal departments and agencies and private sector integrators and suppliers use widely varied ICT SCRM practices. This fact is underscored by the report from the University of Maryland's Supply Chain Management Center, which indicates that there is an overall lack of emphasis on ICT SCRM from companies of all sizes (see Appendix D). As a result, the potential for intentional and unintentional compromise of federal information systems increases.

## 2.2 Success Factors

Solving the challenges associated with ICT SCRM requires integrating practices from information security, software assurance, supply chain assurance, system and software engineering, project management, quality, acquisition, and a number of other disciplines.

SCRM is a multidisciplinary practice with a number of interconnected enterprise processes that, when performed correctly, can acceptably manage the risk of utilizing ICT products and services.

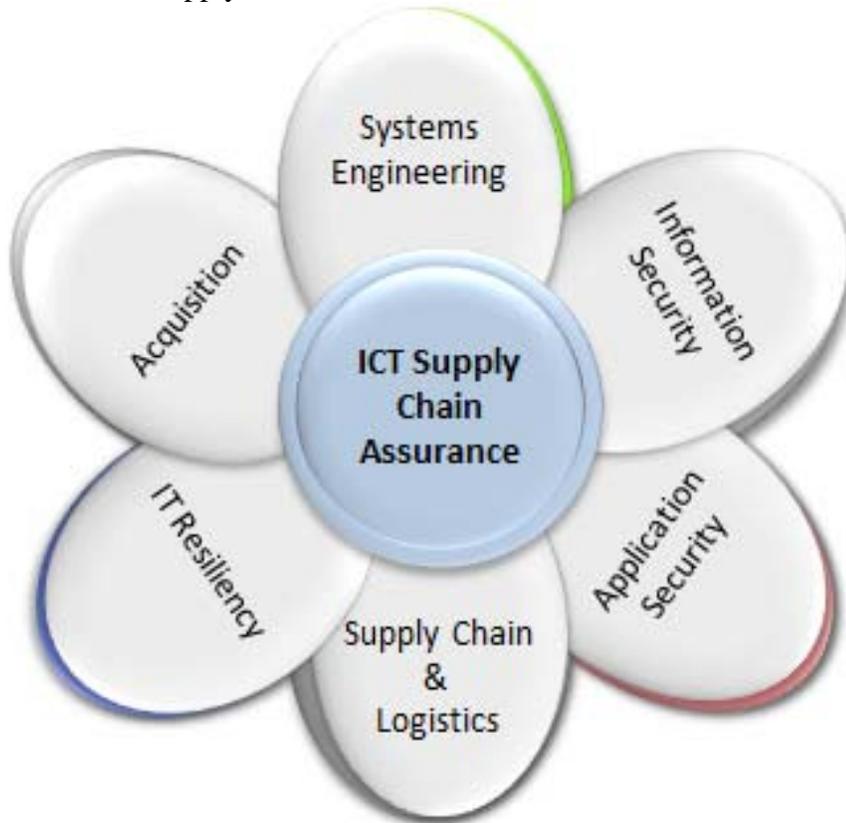
To ensure success of ICT SCRM, organizations need to achieve a certain level of maturity in these multiple disciplines and ascertain that basic, high-level business practices are in place and performing well. For example, organizations can begin improving their understanding and management of ICT supply chain risks simply by ensuring that they understand their cost and scheduling constraints, have integrated information security requirements into the acquisition language, use applicable baseline security controls as one of the sources for security requirements, have a robust software quality control process, and have established multiple delivery routes for critical system elements.

To maximize value from implementing specific ICT SCRM practices described in this document, organizations should first assess certain existing practices and ensure that those practices, as a foundation, are performed well.

Basic, high-level business practices that need to be performed prior to implementing the specific ICT SCRM practices contained in this document include:

- Follow consistent, well-documented, repeatable processes for system engineering, ICT security practices, and acquisition;
- Implement the appropriate tailored set of baseline security controls in NIST SP 800-53 required by the FIPS 199 impact levels;
- Perform quality assurance and quality control;
- Assign roles and responsibilities to specific individuals, including who has the required authority to take action, who has accountability for an action or result, and who should be consulted and/or informed. Ensure 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 in or approve of each milestone decision;
- Ensure adequate resources are allocated for information system security and SCRM – without funding, nothing will happen;

- Develop, implement, and test a contingency plan to include the supply chain to ensure integrity and reliability of the supply chain even during adverse events (e.g., natural disasters such as hurricanes or economic disruptions such as labor strikes). Such plans may incorporate the use of multiple suppliers or multiple supply chains. This includes actively managing suppliers through contracts/Service-Level Agreements (SLAs); and
- Have a robust incident management program which is successful at identifying, responding to, and mitigating security incidents. This program should be capable of identifying causes of security incidents, including those originating from the supply chain.



**Figure 1. Components and Contributing Disciplines of ICT SCRM**

In addition, the multidisciplinary nature of ICT SCRM, illustrated in Figure 1, requires continuous collaboration and coordination by practitioners from multiple disciplines that have distinct bodies of knowledge, lexicons, and vocabularies. Responsibilities for these disciplines and activities normally reside within different entities of an enterprise, necessitating collaboration across organizational boundaries. Although the diagram does not indicate the need for legal, finance, etc., these business functions provide an important dimension to SCRM and should be considered when necessary.

Section 3 of this document discusses ways of facilitating cross-organizational collaboration. Section 4 of this document provides specific ICT SCRM practices which are tailored to address the multidisciplinary view by categorizing the practices under the headings of programmatic activities, general requirements, technical

implementation requirements, and verification and validation requirements. These practices are directed to acquirers, integrators, and suppliers within the ICT supply chain.

DRAFT

### **3 Implementing Supply Chain Risk Management**

Acquiring organizations need an integrated approach to assess and mitigate supply chain risk while balancing associated costs. The development of an organization-wide policy and procedures that outline the roles and responsibilities of all stakeholders is the first step in implementing a SCRM program.

This section provides an approach to establishing a SCRM process within an organization to enable federal departments and agencies to implement SCRM practices and make informed decisions on the assurance of the ICT supply chain when procuring services and operating hardware or software. Federal agencies should share SCRM practices and work with supply chain partners to minimize the impact of divergent requirements. Federal agencies are encouraged also to leverage evidence collected by supply chain partners for other process areas such as security, logistics, or compliance that may be reusable to demonstrate compliance with SCRM.

The collection of SCRM evidence may be considered confidential and/or proprietary, thus requiring protection. Consider including specific language on how the supply chain evidence is handled and by whom during the agreement process. The owner of the supply chain evidence should be allowed to make the decision on how to demonstrate and/or deliver the evidence to the acquirer based on its sensitivity.

Section 3.1 defines the roles and responsibilities that should be defined in an SCRM policy, and Section 3.2 provides guidance on integrating ICT SCRM considerations into federal agency procurements.

Organizations should develop procedures for determining which information systems should implement ICT SCRM mitigation strategies guided by FIPS 199 security categorization, FIPS 200/NIST SP 800-53 security control baselines, and the phase of each individual system life cycle. Note that NIST SP 800-53 provides supply chain protection guidance for information systems at the high-impact level.

#### **3.1 Roles and Responsibilities for Information and Communication Technology Supply Chain Risk Management**

Implementation of ICT SCRM will require an acquiring organization to establish a coordinated team approach to assess the ICT supply chain risk and manage this risk 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.

ICT SCRM roles and responsibilities are distributed among members of a variety of different organizations, including IT, information security, contracting, and legal. Managing the ICT supply chain is an organization-wide activity. Members of the ICT SCRM team should be a diverse group of people who collectively are aware of the challenges associated with the global aspects of ICT supply chain, including an understanding of how ICT products and services are procured and integrated,

familiarity with methods of attack and how to prevent them, as well as legal and procurement aspects of the discipline. The strategies and mitigations proposed by ICT SCRM should comply with the FAR as well as specific organizational policies and procedures.

Note that the specific terms and roles will vary among organizations. In some organizations, a single individual may hold multiple roles.

**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 Office** - The Contracting Office has the authority to enter into, administer, and/or terminate contracts and make related determinations and findings. In the Contracting Office, the Contracting Officer (CO) is responsible for developing an acquisition strategy including technical mitigations which can reduce supply chain risk. The Contracting Officer's Technical Representative (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** - Legal is responsible for advising the team on legal issues related to the acquisition process.

**Risk Executive (Function)** - The Risk Executive Function will work across the organization to ensure consistency in how ICT SCRM considerations are integrated into the organization's overall acquisition strategy and processes. The Risk Executive Function ensures that procurements reflect organizational risk tolerance, and is considered along with other types of risks in order to ensure mission/business success.<sup>6</sup>

**Mission/Business Owner** - The Mission/Business Owner is a high-level official ultimately responsible for the procurement, development, integration, modification, operation, and maintenance of an information system. The Mission/Business Owner may delegate execution of their responsibilities to Program Managers who works closely with the Authorizing Official (AO), Senior Agency Information Security Officer (SAISO), Information Systems Security Officer (ISSO), and the CO to ensure that supply chain risk mitigation strategies are selected, implemented, and operating as intended. The Mission/Business Owner is ultimately responsible for ensuring collaboration with various functional experts to identify and implement ICT supply chain practices that are sufficient to mitigate risks. The functional areas that may be involved include: systems engineering, system security engineering, facilities management including physical security, requirements engineering, quality assurance, reliability, compliance, manufacturing, assembly, testing, acceptance, maintenance, system and network administration, shipping and receiving, packaging and labeling, delivery, inventory management, finance, disposal, and waste management.

---

<sup>6</sup> Adopted from NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

**Chief Information Security Officer (CISO)** - The Chief Information Security Officer, also known as SAISO, is responsible for promulgating policies on security integration in the SDLC and the development and implementation of security policy, guidelines, and procedures pertaining to SCRM. The CISO plays a leading role in introducing an appropriately 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, ensuring that assessments are performed by a third party (not necessarily an external party).

Table 2 summarizes the roles of various ICT SCRM stakeholders with respect to SCRM Capability Implementation described in Section 3.3. The following terms are used in the table to articulate the level of engagements each specific role should have in the process:

- Lead –holds responsibility for decision making and execution of the activity;
- Oversee –provides senior management oversight to the activity and its execution; and
- Advise –provides expert advice to the role that leads the activity.

Process	Risk Executive Function	CIO	CISO	Contracting	Legal	Mission/Business Owner
Plan Procurement	Oversee	Oversee	Oversee	Lead	Advise	Lead
Define/Develop Requirements	Oversee	Oversee	Oversee	Lead	Advise	Lead
Identify Potential Suppliers and/or Perform Market Analysis	Oversee	Oversee	Oversee	Advise	Advise	Lead
Complete Procurement	Oversee	Oversee	Approve	Lead	Advise	Lead
Operations and Maintenance	Oversee	Oversee	Oversee	Advise	Advise	Lead

**Table 1 ICT SCRM Stakeholders**

### 3.2 Information and Communication Technology Supply Chain Risk Management Implementation Process

Reasonable risk taking is appropriate as long as risks are controlled and mitigated. This section describes the activities that take place to mitigate supply chain risk during the life cycle of the project using NIST SP 800-53.

It should be noted that the practices dedicated to mitigating supply chain risks for individual acquisitions should be commercially reasonable, and the resources used should be commensurate with the magnitude and criticality of systems and/or elements being procured. For the purposes of ICT SCRM only those elements that contain programmable logic and that are critically important to the system function should be evaluated for ICT SCRM risks. Furthermore, not every element is critical, whether it is a chip, a router, or a piece of software. Agencies should conduct an analysis to support a risk-based decision as to whether to apply all, some, or none of the practices described in this document based on the criticality of components to information system functionality. Draft NIST SP 800-53 Rev4 SA-14 and SA-15 (enhancement 3) provide further information on determining criticality of system components.

Prior to entering into a contract for ICT, an agency should analyze the risks, benefits, and costs associated with implementing SCRM requirements. Since managing supply chain evidence collection, processing, and protection can result in exponential administrative costs to acquirers, integrators, and suppliers, clearly defining these requirements is critical. ICT SCRM concerns should be carefully balanced with programmatic concerns including required resources (i.e., cost, performance, and schedule), functionality, and security.

For federal systems, NIST SP 800-53 should be used as the starting point for determining the set of applicable security controls for an information system (for the security control baseline). Not every information system acquisition is a candidate for assessing supply chain risk or incorporating supply chain mitigation language into procurement documents. For example, 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.

Therefore, for FIPS 199 high-impact systems, ICT SCRM should be explicitly integrated into the acquisition process to analyze potential supply chain risks and implement additional security controls and/or SCRM practices as needed, depicted by a solid line and in red in Figure 2.

In the case of information systems categorized at the FIPS 199 moderate- or low-impact level, NIST SP 800-53 implementation of SA-12 is not required. For moderate-impact systems, a *risk-based decision* should be made by *an authorizing official* as to whether ICT SCRM is warranted (depicted by a dash line and in yellow in Figure 2). Low-impact systems do not require significant ICT SCRM attention, depicted in green in Figure 2.

(Note: Since IA controls are a living document, the most current version of SA-12 should be reviewed to make the determination.)

Figure 2 represents the integrated ICT SCRM Implementation Process described in the following sections.

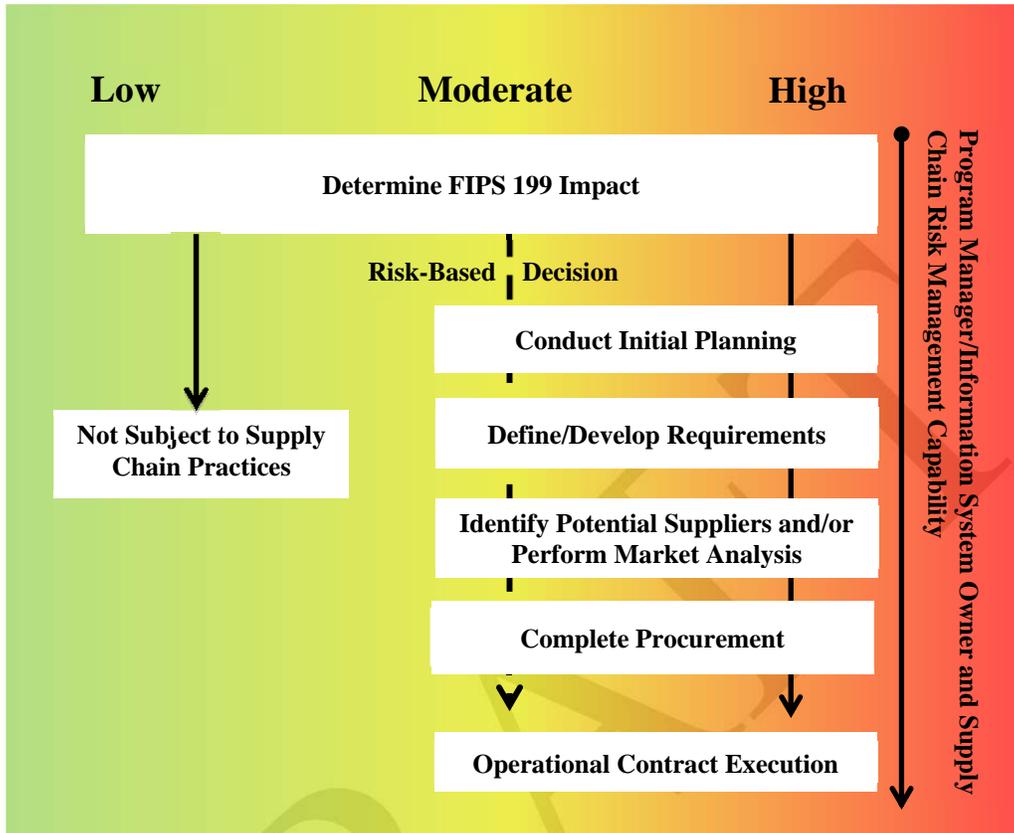


Figure 2 – ICT SCRM Implementation Process

### 3.2.1 Determine Risk/Impact

Mission/business owners, information system security personnel, stakeholder representatives, and possibly outside experts should identify applicable supply chain risks. Contracting and program office officials are jointly responsible for assessing, monitoring, and controlling risk when selecting projects for investment and during program implementation. There are several methods of compiling potential risks including reviews of current and historical project documentation, brainstorming, interviewing of stakeholders, checklists, marketing analysis, supplier-specific risk assessment, and standard operating procedure (SOP) review. Risks to be identified and compiled are known chronic risks, such as product/element risks that are persistent rather than transient risks. Appropriate techniques should be applied to manage and mitigate risk during the acquisition of information technology. Techniques include, but are not limited to: prudent project management; use of modular contracting; thorough acquisition planning tied to budget planning by the program, finance, and contracting offices; continuous collection and evaluation of risk-based assessment data; prototyping prior to implementation; post-implementation reviews to determine

actual project cost, benefits and returns; and focusing on risks and returns using quantifiable measures.

Mission/business owners or designee, in consultation and coordination with advisors and decision makers (e.g., technical leads, contracting officer, and legal counsel), should identify a set of ICT SCRM-related requirements and controls. Section 4 of this document provides a set of practices that can be used as a source for creating SCRM-related requirements.

### **3.2.2 Conduct Initial Planning**

The procurement official (under the Contracting role in Section 3.1), with the assistance from the mission/business owner or their designee, information security experts, legal counsel, and other applicable members of the ICT SCRM team should modify or develop a procurement strategy (e.g., Acquisition Plan) to best support the selected project/program. To help identify and plan for addressing ICT supply chain risk, the acquisition plan should include:

- A list of potential sources of supplies/services that could meet the need; the extent and results of market research, applicable threat analysis, and the impact of these sources 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; e.g., request for information (RFI) activities, source sought, market surveys;
- A description of various contracting considerations, including contract type and the use of performance-based contracts; e.g., requests for quotation (RFQ), requests for proposal (RFP), Cooperative Research and Development Agreements (CRADAs), grants, and similar documents (See Part 16 of the FAR for a description of different contract types.);
- Information security and supply chain risk mitigation strategies and practices are based upon the (known) potential suppliers/service providers that could meet the program requirements, and the impact suppliers may have on various systems and element;
- Identification and application of relevant acquisition policies and contract clauses to ensure that the needed authorities are in place and sufficient to verify the element, the element processes, and the business processes of the acquirer and supplier; and
- Description of procurement roles and responsibilities, a roadmap for completing procurement actions and milestones, and a discussion for including special ICT SCRM considerations in the purchase and implementation of products and/or services.

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.)

### **3.2.3 Define/Develop Requirements**

The mission/business owner or their designee, with assistance from the procurement official and other members of the SCRM team, if applicable, should define and document requirements for the procurement. During this process, mission, functionality, quality, and security requirements should be developed and documented. This process will identify the requirements for the procurement and how these requirements will apply to the specific items of supply (elements and processes).

Not every information system acquisition is a candidate for assessing supply chain risk or incorporating supply chain mitigation language into contract documents. For information systems categorized at the FIPS 199 low-impact level, ICT SCRM controls and enhancements are not specified. In the case of systems at the moderate-impact level, it is up to the AO to make a risk-based determination whether SCRM is required using the security controls moderate baseline as guidelines. NIST SP 800-53, Rev. 4, Appendix F, Security Control Catalog, specifies ICT SCRM controls and enhancements for information systems categorized at the FIPS 199 high-impact level.

### **3.2.4 Identify Potential Suppliers and/or Perform Market Analysis**

Once the requirements are defined, the mission/business owner should initiate a market review for potential suppliers. This effort includes market analysis, publication of an RFI or Sources Sought Notice (SSN) and review of the responses, initial threat analysis, and down-selecting integrators/suppliers. It should be noted that not all circumstances warrant publication of an RFI or an SSN. It is up to the acquirers to select specific approaches to individual procurements.

#### **Develop and Publish Market Analysis/Assessment**

Mission/business owners should perform market analysis using one or more of the following methods: publishing a SSN, publishing a RFI, or performing a market survey to obtain prices from potential suppliers.

Mission/business owners or their designees should identify known and potential sources of supply (including qualified integrators/supplier and qualified product lists). If the potential integrators/suppliers are not known, the mission/business owner or designee should work with the contracting officer to do a market analysis to identify alternative integrators/suppliers with their supply chains. The market analysis should identify which companies can provide the required elements or services and suggest 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. Mission/business owners should be aware that respondents may include integrators/suppliers not previously identified.

As part of the due diligence efforts, market analysis questionnaires (such as the UMD Study in Appendix D) can assist acquirers in obtaining additional information about the system/element, system/element processes, as well as the supplier/system integrator organizations. The due diligence involves taking all “reasonable steps” necessary to ensure that the system not only meets business and technical requirements, but also addresses ICT SCRM concerns. The responses to the due diligence questionnaires will inform acquirers of potential risks associated with the elements or services they are considering for purchase and the suppliers SCRM practices. When using the questionnaires, acquirers should request evidence or may coordinate an on-site follow-up that reviews objective evidence of the provided answers where appropriate and evaluates them for potential risks or red flags. These questionnaires should be used as tools and not checklists or complete listings of all possible concerns.

As a part of market analysis, an organization may choose to publish an RFI or a SSN to give integrators and suppliers an opportunity to tell their story based on the description in the RFI/SSN.

**Review Request for Information Responses**

This activity involves creating a plan for evaluating responses and the criteria to be used to evaluate them. The evaluation plan describes the process by which market analysis data/information should be secured and evaluated against the criteria, including the time frame for the evaluation and any measures that can be used to support the evaluation process. The results can then be used to help determine the best candidate for the acquisition. It is imperative that qualified supply chain and/or information security professional(s) are included in the process to evaluate the ICT supply chain criteria. The evaluation may be administered through both qualitative and quantitative methods to provide a consistent methodology for choosing integrators/suppliers. In the case where a response does not meet the criteria, the response is normally eliminated from future consideration.

ICT SCRM-focused evaluation criteria can be applied to both integrators and suppliers and should include the following categories:

Category	Description
<p><b>Organization (integrator/supplier)</b></p>	<p><b>Key aspects of the integrator/supplier organization.</b>                      Identifying and gathering information on the supplier/integrator organization is critical to managing supply chain risk. Examples of such information include:</p> <ul style="list-style-type: none"> <li>• Organizational History – years of operation, Central Contractor Registry (CCR) registration record</li> <li>• Foreign Interests and Influences (including ownership)</li> <li>• Financial History and Status – Size of Organization, credit rating (including Dun and Bradstreet [DUNS] record)</li> <li>• Facilities: Development, operational, associated policies</li> </ul>
<p><b>Element Processes</b></p>	<p><b>Robustness and completeness of life cycle processes applied to elements and services to be procured.</b>                      Effectively applied supply chain and ICT SCRM processes</p>

	<p>decrease the likelihood of both intentional and unintentional supply chain weakness that can lead to exploitable vulnerabilities. Element processes that should be addressed run the full element life cycle and can start at the concept phase and go through to disposal. Examples of these processes may include:</p> <ul style="list-style-type: none"> <li>• Concept and Planning</li> <li>• Architecture and Design</li> <li>• Development</li> <li>• Integration/Assembly</li> <li>• Assessment, Evaluation, and Testing (including the evaluation of the tools used in the process)</li> <li>• Manufacture and Packaging</li> <li>• Delivery</li> <li>• Acceptance and Installation.</li> <li>• Support Services</li> <li>• Operating Environment</li> <li>• Disposal</li> </ul>
<p><b>Elements</b></p>	<p><b>Element’s security track record.</b>                  Elements are subject to both intentional and unintentional insertion of malicious functionality, weaknesses, and counterfeits. Some key items addressed as part of the element evaluation should include:</p> <ul style="list-style-type: none"> <li>• Architecture/Design characteristics – including built-in defenses and whether they meet functional requirements.</li> <li>• Element history and licensing – reviewing element quality, reliability, security incidents, licensing terms, indemnifications, etc.</li> <li>• Public record of the number of vulnerabilities associated with the element and the process for addressing incidents, root cause analyses, and fixes.</li> </ul>

**Table 3. Evaluation Criteria**

**Conduct Security, Threat, and Vulnerability Assessment**

Security, threat, and vulnerability assessment should be conducted as a part of the RFI review. At this point in the evaluation process, this assessment should be conceptual and high-level, and should identify obvious issues that do not require a detailed analysis. The criteria for this assessment should be defined using mission, functional, quality, and security requirements. Data to support this assessment should be collected from a variety of sources, such as:

- Integrator/supplier security track record;
- Individual threat and malicious behavior affecting supply chain environment or the element;
- Software security training and awareness within the integrator/supplier organization;

- Security monitoring both of the element and element processes;
- Timeliness of vulnerability mitigation of element and element processes;
- Policies for service confidentiality;
- Policies for information sharing and access control;
- Policies for integrator/supplier information security;
- Results of independent third-party evaluations; and
- Results of security certifications.

### **Down Select to Qualified Vendors**

Once responses are evaluated and the threat assessment is conducted, the acquirer should select a qualified set of integrators and suppliers who have the capacity to participate in the specific procurement. Results of the threat assessment should be used to down select vendors.

### **3.2.5 Complete Procurement**

After the completion of market analysis, the organization should develop a statement of work (SOW) and statement of objective (SOO) for the release of an RFP or RFQ. If the organization published an RFI or an SSN and based on that selected a specific set of integrators/suppliers, this RFP/RFQ should be issued to this group of integrators/suppliers.

#### **Develop and Publish Request for Proposal/Request for Quote**

The mission/business owner or designee should develop a SOW/SOO that includes a detailed description of the specific functional, technical, quality, and security requirements and qualifications. This document should include the selected ICT SCRM practices (general and technical requirements, and validation and verification activities) and NIST SP 800-53 controls relevant to an integrator and in some instances, a supplier supporting acquirer activities. Requirements developed for market analysis and any adjustments made from the results of the RFI process should provide significant input to the RFP or RFQ.

The following should be considered when developing the SOW/SOO requirements:

- Appropriate level of risk distribution among the acquirer, integrator, and supplier. SOW/SOO should state integrator's and supplier's level of responsibility for supplying assurance for systems and elements;
- Use of 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 integrator/supplier to reduce vulnerabilities, and what past vulnerabilities indicate about product/service strength, speed of patching, integrator/supplier pattern of addressing identified vulnerabilities, and current known yet unfixed vulnerabilities. (Note that suppliers may weigh need to know for release of

information about existing, but unfixed vulnerabilities against risk of exploitation of their products.) Since past performance is no guarantee of future result, recent major changes in the integrator/supplier organization that might invalidate past performance should be examined;

- Requirements for processes (including test and evaluation [T&E] processes) and inclusion of these processes in contract documents;
- The methodology used by integrators to select/manage their suppliers and whether the integrator/supplier imposes similar requirements on their downstream suppliers;
- Requirement for respondents to provide an ICT SCRM Plan that addresses, in detail, their internal and external practices and controls employed to minimize the risk posed by counterfeits/grey market elements, and known and unknown vulnerabilities in systems, elements, and services. In this plan, the respondents should address the implementation of foundational enterprise practices addressing logical and physical aspects of enterprise operations, and identify how they have integrated ICT SCRM perspective into these practices; and
- How acquirer's and integrator's/suppliers proprietary data will be used, how long it will be kept, with whom it can be shared, and what intellectual property protections will prevail.

The SOW/SOO needs to be a very clear and concise document and include performance measures, evaluation criteria, and thresholds against which the respondents will be measured.

### **Review Request for Proposal/Request for Quote Responses**

Once the integrator responds to the SOW/SOO and presents a proposal, the acquirer will review the response. This review requires participation of multiple stakeholders who will address multiple facets of the response. The mission/business owner or designee will review adherence to procurement objectives. Appropriate technical experts will conduct a technical review. The Contracting Officer will conduct the cost review. Other team members will review other portions of the response to ultimately determine which proposal is the most beneficial (best value) to the government.

The review team will evaluate the quality of each integrator response against predetermined, weighted evaluation factors to gauge the quality of each proposal. The review team will look for documented evidence of an integrator's claims to meet the desired ICT SCRM requirements and other indicators. Documentation can include 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 business relations.

### **Complete Security Threat and Vulnerability Assessment**

A more detailed assessment of the integrator's proposal should be conducted, similar to the assessment during RFI review, but at a greater level of fidelity and granularity. The criteria noted in the section describing such evaluation of RFI responses should be

used as a starting point. Other items may be added to the evaluation as appropriate, and the evaluation should be conducted with the increased rigor and specificity of collected and evaluated data.

### **Contract Negotiation and Contract Award**

The evaluation results in the selection of the best proposal(s) for contract negotiation. During negotiations, the acquirer(s) and integrator(s) negotiate on requirements, terms, and conditions. It is important that the negotiation conducted at this point in time does not compromise the ultimate ICT SCRM goals in support of the acquirer's mission requirements. It should be noted that integrators may question the ICT supply chain assurance requirements because they may not be comfortable with this new specialized set of requirements and the risk they may need to assume to fulfill these requirements. Acquirers may find that integrators may bid too high because of perceived complexity and unanticipated investment related to complying with new ICT supply chain assurance requirements.

Acquirers should consider share-in-savings arrangements (savings as a result of implementing supply chain assurance requirements as stated in agreement). The sharing includes not only costs and benefits but also the willingness to afford the supplier more time to engage in the education and training that is needed. An alternative would be to consider a contract type that shifts some of the risk to the acquirer and/or provide additional cost or performance incentives (see FAR Subpart 16.1 and FAR Subpart 16.3 for incentive contracts). Negotiated agreements are sometimes overlooked when drafting the final contract award. Therefore, when awarding the contract, acquirers need to ensure that all SCRM agreements made during negotiation are incorporated into the contract when it is awarded.

### **3.2.6 Operational Contract Execution**

Once a system becomes operational, the operating environment may change. Changes include, but are not limited to, suppliers, elements, delivery processes, and business processes. These changes may alter, add, or reduce ICT supply chain risks. During operations, acquirers should continue to perform ICT SCRM, including the assessment of foundational enterprise practices. The acquirer will need to ensure that the integrator/supplier understands supply chain risk and provides information on applicable changes to the element, environment, vulnerabilities, and patches on an ongoing basis. The following activities will help the acquirer maintain supply chain oversight and improve processes for future procurements:

- Collect, analyze, record, and disseminate ICT SCRM lessons learned within the project and within the larger organization(s). This information will help enhance immediate project performance and provide input into the enterprise ICT SCRM process;
- Collect information on whether the compromises that were made during the procurement with regards to mitigating ICT supply chain risks substantially increased that risk;
- Identify gaps that were not addressed in past projects and how they can be filled;
- Monitor and periodically (or continuously if appropriate) reevaluate changes in the risk environment including technology innovation, operational

environment, regulatory environment, etc. Respond to change where appropriate through modifying ICT SCRM requirements or if needed modifying relationships with integrators/suppliers. 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 integrator/supplier;

- Integrate ICT SCRM considerations in continuous monitoring activities; and
- Collect feedback on integrator/supplier responsiveness and effectiveness at mitigating risks per acquirer requests.

The acquirer should use the Key Practices (KPs) in Section 4 to address supply chain assurance when acquiring replacement components or field additions/modifications/upgrades, particularly if they do not go through traditional acquisition processes that examine ICT supply chain risks.

Acquirers and integrators need to be aware of the time frame within which when their elements and systems become obsolete and plan for replacing and upgrading these elements and systems. Systems that have a long life cycle may require a substantial number of elements that are no longer available from the original component manufacturer or through their franchised distributors. Acquirers and integrators should plan for when elements become obsolete.

DRAFT

## 4 Supply Chain Risk Management Practices

This section provides ten practices that an acquiring 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 implementation requirements. The programmatic and validation/verification activities are implemented by the acquiring organization.

The term “acquirer” is used to mean the federal organization acquiring the product or service. The term “integrator” is used to depict an organization that specializes in customizing (e.g., combines, adds, optimizes) elements, processes, and systems. The integrator functions can be performed by acquirer, integrator, or supplier organizations. The term “supplier” is used to depict an organization or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain. The term is synonymous with vendor and manufacturer, and in this document also applies to maintenance/disposal service providers. The term “element” is used throughout to mean 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.

Appendix A provides a glossary of terms used throughout the document.

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. It should be noted that, in some cases, activities, functions, and practices may overlap. Organizations should use the guidance in this document to develop a strategy that best meets their needs. Table 4 describes how the practices are formatted by role, activities, and requirements.

It is recognized that the rapid pace of change in ICT requires all actors to continuously use, modify, improve, and redevelop their technologies, products, and services to maintain the highest levels of security. Therefore, every effort is made in the practices to identify essential characteristics, actions, or processes and not specific technologies or methodologies. These practices are harmonized with existing and emerging international consensus-based standards and point to those as appropriate throughout the section. Federal departments and agencies are reminded that U.S. law and policy require them to use international, voluntary consensus standards in their procurements, except where inconsistent with law or otherwise impractical,<sup>7</sup>

---

<sup>7</sup> “National Technology Transfer and Advancement Act,” “Office of Management and Budget (OMB) Circular A-119 Revised: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities,” and Trade Agreements Act of 1979, as amended.

The ten practices, if implemented in their entirety, cover the complete SDLC.

- 4.1 Uniquely Identify Supply Chain Elements, Processes, and Actors
- 4.2 Limit Access and Exposure within the Supply Chain
- 4.3 Create and Maintain the Provenance of Elements, Processes, Tools, and Data
- 4.4 Share Information within Strict Limits
- 4.5 Perform SCRM Awareness and Training
- 4.6 Use Defensive Design for Systems, Elements, and Processes
- 4.7 Perform Continuous Integrator Review
- 4.8 Strengthen Delivery Mechanisms
- 4.9 Assure Sustainment Activities and Processes
- 4.10 Manage Disposal and Final Disposition Activities throughout the System or Element Life Cycle

The practices are not listed sequentially, in order of importance, or aligned with system or element life cycle phases. The five Foundational practices listed in Section 2 are provided first, with the other five practices to follow. The ten practices are descriptive and do not impose a specific approach or implementation. These practices can be applied at any point in the system or element life cycle.

Several SCRM practices can be simultaneously applied to an information system or elements of an information system. In certain instances or with information systems, different practices may be applied during multiple phases or 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 4 reflects the types of actions and the descriptions an Acquirer, Integrator, and Supplier would implement for each SCRM practice selected. The Business/Mission Owner or a designee along with information security experts should determine if the practices selected are sufficient to mitigate supply chain risks. The business owner 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.

All of the tools and mechanisms described in this section that help implement the key practices should be protected throughout the system or element life cycle.

<b>Role</b>	<b>Type of Action</b>	<b>Description of Action</b>
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 programs that are either in response to contractual requirements or to document existence of programmatic activities that reduce supply chain risk.
Supplier	General Requirements	General practices that a supplier will implement within programs to document existence of programmatic activities that reduce supply chain risk.
Integrator	Technical Implementation Requirements	Detailed technical practices that an integrator will implement within programs to document technical capabilities to manage supply chain risk.
Supplier	Technical Implementation Requirements	Detailed technical practices that a supplier will implement within programs to document technical capabilities to manage supply chain risk.
Acquirer	Validation and Verification Activities	Suggestions for how an acquirer can ascertain that integrators or suppliers have implemented ICT SCRM.
Integrator	Validation and Verification Requirements	Suggestions on how an integrator can demonstrate that they have implemented ICT SCRM.
Supplier	Validation and Verification Requirements	Suggestions on how a supplier can demonstrate that they have implemented ICT SCRM.

**Table 4. Practice Format**

When acquiring organizations are determining their IT 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, 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.<sup>8</sup>

#### **4.1 Uniquely Identify Supply Chain Elements, Processes, and Actors**

Knowing who and what is in an enterprise's supply chain is critical to gain visibility into what is happening within it, as well as monitoring and identifying suspicious or adverse events and activities. Without knowing who and what are in the supply chain, it is impossible to determine what happened, mitigate the incident, and prevent it from

<sup>8</sup> NIST SP 800-53 provides a set of controls that address supply chain risk assurance which are targeted for information assurance professionals for the purposes of achieving certification and accreditation. Given a designation AO requires the application of these controls, the Certification and Accreditation or 800-53 compliance of either an element or outsourced IT infrastructure is possible.

happening again. Uniquely identifying organizations, personnel, mission and element processes, communications/delivery paths and elements, and components and tools used on them establishes a foundational identity structure for assessment of ICT supply chain activities. Everything and everyone that participates in the supply chain should also be uniquely identifiable so that activities can be traced and responsible actors and entities defined (traceability). For example, labeling and tagging software packages and modules, hardware devices, individual elements, and processes that surround them will allow acquirers, integrators, and suppliers will aid in better understanding activities that have occurred (visibility) and manage any emerging risks.

#### **4.1.1 Acquirer –Programmatic Activities**

- a) Establish and retain unique identification (physical and logical) of roles, organizations, people, ideas, requirements, processes, items of supply, tools used on items of supply, T&E procedures, delivery mechanisms, support mechanisms, and disposal/final disposition activities at the lowest practicable level.
- b) Require that unique identifiers and methods of identification be difficult or impossible to alter and that any alterations adhere to previously set, clearly defined criteria.
- c) Require that identification methods are sufficient to support provenance in the event of a supply chain issue or adverse supply chain event.
- d) Use threat response practitioners to assist the systems engineering and the implementation, oversight, and compliance communities in addressing potential or documented deficits or faults in the implementation of unique identities to enhance the ability of all supply chain participants to monitor the supply chain for adverse events.
- e) Document that individuals are assigned appropriate roles throughout the supply chain and system/element life cycle, regardless of personnel turnover, to ensure that the visibility of critical processes and elements is maintained.

#### **4.1.2 Integrators – General Requirements**

- a) Ensure the identification method is sufficient to support system/element provenance in the event of a supply chain issue or adverse supply chain event.
- b) Ensure the implementation of unique identification requirements by developing and applying policies, procedures, and means to identify objects and activities within the supply chain at the sub-element, element, and system levels.
- c) Apply unique identification requirements to design, test, and evaluation activities to include design tools (hardware and software), drawings and diagrams, and tools used to protect the design, test, and evaluation processes.
- d) Implement unique identification requirements in all written supplier agreements.
- e) Require strength of the authentication mechanism to be commensurate with the significance of the element, system, process, and/or organization to mission requirements.

- f) Define, design, and implement roles to limit privilege so that the roles being performed do not result in adverse consequences throughout the supply chain and element life cycle.
- g) Establish mechanisms and processes for checking and auditing unique identifications. Any deficiencies should be noted and corrected.
- h) Document that individuals are assigned appropriate roles throughout the supply chain and system/element life cycle, regardless of personnel turnover, to ensure that the visibility of critical processes and elements is maintained.

#### **4.1.3 Suppliers -- General Requirements**

- a) Ensure that identification methods are sufficient to support provenance in the event of a supply chain issue or adverse supply chain event.
- b) Document the application of unique identification requirements applicable to design, test, and evaluation activities to include design tools (hardware and software), drawings and diagrams, and tools used to protect the design, test, and evaluation processes.
- c) Require that the strength of the authentication mechanism is commensurate with the significance of the element, system, process, organization, and mission requirements.
- d) Define, design, and implement roles that limit privilege and create redundancy throughout the supply chain and element life cycle so that no single role can, intentionally or unintentionally, create adverse consequences.
- e) Require protection and safeguarding of authenticators.

#### **4.1.4 Integrators – Technical Implementation Requirements**

- a) Implement unique identification requirements by applying policies, procedures, and means of identification to objects and activities within the supply chain at the device, sub-element, element, system and system levels.
- b) Apply unique identifiers to design, test, and evaluation activities, including design tools (hardware and software), drawings and diagrams, and tools used to protect the design, test, and evaluation processes.
- c) If two or more unique identities have access to an element, process, organization, information, or system, use multifactor authentication mechanisms. Two or more unique identities can include one user and one administrator.
- d) Limit the use of a unique identity for multiple uses by restricting privileges and permissions (e.g., system single sign-on, Personal Identity Verification implementation).
- e) Employ FIPS-validated or National Security Agency (NSA)-approved cryptography to implement signatures.
- f) 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.

#### **4.1.5 Suppliers – Technical Implementation Requirements**

- a) Document that all unique identification requirements are implemented by applying policies, procedures, and means of identification to objects and activities within the supply chain at the device, sub-element, element, and system levels.
- b) Document that unique identifiers were established to track the design, test, and evaluating activities, which include design tools (hardware and software), drawings and diagrams, and tools used to protect the design, test, and evaluation processes.
- c) Document the use of multifactor authentication mechanisms, if two or more unique identities have access to an element, process, organization, information, or system. Two or more unique identities can include one user and one administrator.
- d) Employ FIPS-validated or NSA-approved cryptography to implement digital signatures.

#### **4.1.6 Acquirer – Validation and Verification Activities**

- a) Assess the effectiveness of acquirer and integrator identity management and access control policies, procedures, and practices in limiting exposure of, or access to, elements or element processes.
- b) Monitor the acquirers' and integrators' internal controls over the assignment of tasks and activities to roles.
- c) Perform audits on unique identification deficiencies and report up the supply chain for corrective action.
- d) Ensure that unique identifications are assigned to all actors/roles and to the tactics, techniques, procedures, and tools most associated with those actors in order to facilitate detection and tracking of threats across multiple supply chains.
- e) Employ tools and techniques to determine if authenticators are sufficiently strong to resist attacks intended to discover or compromise authenticators (including, but not limited to, penetration testing tools and techniques and Intrusion Prevention System [IPS]/Intrusion Detection System [IDS] tools).
- f) Check for robustness of the infrastructure that manages unique identities. Assess whether identities can be detected or altered (e.g., counterfeiting of credentials or spoofing of identity).
- g) Examine and document weaknesses and vulnerabilities in the unique identity implementation so they may be monitored for adverse events.
- h) Examine and test mechanisms for applying unique identification to discover potential deficits and/or faults in the design or implementation of such mechanisms.

#### **4.1.7 Integrators – Validation and Verification Requirements**

- a) Continuously-monitor internal controls addressing the allocation of tasks and activities to roles. Any changes should be alerted to the user, user management, and network system administrator.
- b) Ensure that unique identifications are assigned to all actors/roles and to the tactics, techniques, procedures, and tools most associated with those actors in order to facilitate detection and tracking of threats across multiple supply chains.
- c) Examine and test mechanisms for the application of unique identifications to discover potential deficits and/or faults in the design or implementation of such mechanisms.
- d) Document weaknesses or vulnerabilities in the unique identification implementation to enhance the ability of all supply chain participants to monitor the supply chain for adverse events.
- a) Report deficiencies up the supply chain for corrective action to ensure that requirements for unique identification are fulfilled.

#### **4.1.8 Suppliers – Validation and Verification Requirements**

- a) Monitor the internal controls addressing the allocation of tasks and activities to roles.
- b) Demonstrate ability to assign unique identifications to relevant actors/roles and the tactics, techniques, procedures, and tools most associated with those threat sources to facilitate detection and tracking of threats across multiple supply chains.
- b) Report deficiencies discovered in critical elements (per acquirer/integrator) up the supply chain for corrective action to ensure requirements for unique identification are fulfilled.

### **4.2 Limit Access and Exposure within the Supply Chain**

Elements that traverse the supply chain are subject to access by a variety of actors. It is critical to limit such access to only as much as necessary for those actors to perform their role(s) and to monitor that access for supply chain impact. Access control privileges can be defined with appropriate granularity in such a manner that only appropriate actors are permitted to monitor or change supply chain elements, element processes, organizations, organizational processes, information, communications, and systems covering the comprehensive supply chain.

#### **4.2.1 Acquirer - Programmatic Activities**

- a) Establish an internal policy for the broad responsibilities of assigning access control to information, systems, supply chain elements, element processes, as well as key personnel and organizational activities as deemed necessary to

- protect the confidentiality, integrity, and availability of supply chain elements and processes throughout the acquisition life cycle.
- b) Instantiate general criteria by which access controls are to be applied, the objects of such controls, the initiating and terminating events or conditions under which such controls are applied, and specific access control mechanisms (e.g., automated, manual, or hybrid).
  - c) Identify the individuals [roles] and organizations with responsibility for the design, development, and implementation of access controls, to include use of information security, operations security, physical security, industrial security, and information assurance (IA) tactics, techniques, procedures, and tools.
  - d) Define requirements to include access control (both physical and logical) requirements in all written agreements with integrators including:
    - Responsibilities for assigning access control among all parties,
    - Mandatory, recommended, and prohibited access control methods; and
    - Audit plans for access control review.
  - e) Define, design, specify, and require assigned roles throughout the supply chain and system or element life cycle so that no single role can, intentionally or unintentionally, create adverse consequences.
  - f) Evaluate all positions for opportunities to expose elements, processes, systems, or information, including requirements to potential compromise.
  - g) When developing requirements, minimize exposing the uses of systems and elements, as well as the processes by which they are designed, developed, produced, tested, delivered, or supported.
  - h) Establish an internal policy for remote access, including allowing access to the organization's location and third-party locations, removable media, network, and other items to be determined.
  - i) Establish and document a policy describing allowed methods of remote access to elements, systems, processes and organizations.
  - j) Establish and enforce requirements for personnel security reviews and assessments for acquirer personnel. These reviews and assessments should include personnel who have exposure or access to elements, element processes, or business activities. Special attention should be paid to those personnel with the technical knowledge or understanding of enterprise processes that would allow them to obtain unauthorized exposure of, or access to, elements or processes that could result in compromise or loss.

#### **4.2.2 Integrator - General Requirements**

- a) Define requirements to include access control (both physical and logical) requirements in all written agreements with acquirers and suppliers including:
  - Responsibilities for assigning access control among all parties;
  - Mandatory, recommended, and prohibited access control methods; and
  - Audit plans for access control review.
- b) Review trade-offs regarding cost, schedule, and performance resulting from the application of different combinations or specific access control mechanisms.
- c) Limit access to the following information (including any associated 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, and 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).

- d) Conduct personnel security reviews and assessments. These reviews and assessments should include personnel who have exposure or access to elements, element processes, or business activities. Special attention should be paid to those personnel with the technical knowledge or understanding of enterprise processes that would allow them to obtain unauthorized exposure of, or access to, elements or processes that could result in compromise or loss.

#### **4.2.3 Supplier – General Requirements**

- a) Document access control mechanisms that limit access to the following information: the identity of the user or developer; the functions of the system; the other systems it will interface with; and when or where the system elements will be acquired. When more information is shared, use other practices in this document to reduce risks.

#### **4.2.4 Integrator – Technical Implementation Requirements**

- a) Develop and implement roles throughout the supply chain and system life cycle to limit opportunities and means available to individuals performing these roles to expose elements, processes, systems, or information, including requirements to potential compromise.
- b) Employ automated and repeatable mechanisms to facilitate monitoring and controlling:
  - a. Various access methods (physical and logical);
  - b. Access occurring with no manual observers and controllers; and
  - c. High volume of access requested in a given short period of time or simultaneously.
- c) Employ automated and repeatable mechanisms to facilitate the maintenance and review of access records.
- d) Maintain records of all physical and logical accesses, both authorized and unauthorized, including by visitors and regular individuals.
- e) Maintain records of any combination of physical and logical activities initiated by both authorized and unauthorized individuals.
- f) Provide access control protection for both remote and mobile devices and the use of remote and mobile access points to the supply chain infrastructure.
- g) Evaluate the sequence by which roles and tasks are performed so that no combination permits undetected or unmonitored performance of tasks or activities.

#### **4.2.5 Supplier – Technical Implementation Requirements**

- a) Document the application of different combinations or specific access control mechanisms within the supply chain.
- b) Document the implementation of any access control protections for both remote and mobile devices, and the use of remote and mobile access points in the supply chain infrastructure.
- c) Document the implementation of key 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.
- d) Document that individuals are assigned to roles in a manner that limits the opportunities or means to cause adverse consequences, throughout the supply chain and life cycle.
- e) Document the instantiation of audit mechanisms used to audit access control procedures (e.g., audit logs, access reports, and security incident tracking reports).

#### **4.2.6 Acquirer - Validation and Verification Activities**

- a) Assess security risks to physical and logical access controls intended to prevent unauthorized exposure of, or access to, tools, processes, people, and systems in the supply chain that create supply chain elements or information about such elements.
- b) Perform security checks at the physical and logical boundary of the element, element processes, facilities, and system, for unauthorized access to or export of information, elements, tools, and materiel used in element processes.
- c) Prevent, detect, and document any physical tampering or altering of access control mechanisms.
- d) Review the integrator's processes and procedures aimed at limiting exposure of system and elements uses.

#### **4.2.7 Integrator - Validation and Verification Requirements**

- a) Demonstrate that a mix of personnel, physical, and logical access controls are implemented which provide a level of protection commensurate with the sensitivity/criticality of the services provided or the elements procured.
- b) Perform technical and procedural audits of mechanisms used to shield information related to elements, including uses, requirements, and metadata.
- c) 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 element or associated information including uses of element.
- d) Assess the effectiveness of alternative configurations in protecting access of elements, processes, systems, and information for the purposes of confidentiality, integrity, and availability.
- e) Continuously monitor internal controls addressing the allocation of tasks and activities to roles.
- f) Test internal access controls for the ability to detect anomalous behavior and facilitate timely intervention to prevent or reduce adverse consequences.

#### **4.2.8 Supplier – Validation and Verification Requirements**

- a) Demonstrate the instantiation and implementation of access control mechanisms across the system or element life cycle and the associated supply chain.
- b) Demonstrate ability to intervene in a timely manner to prevent or reduce adverse consequences within the supply chain.
- c) Provide reports of periodic audits performed in support of access control requirements defined in the agreement document with the acquirer.

### **4.3 Create and Maintain the Provenance of Elements, Processes, Tools and Data**

All system elements originate somewhere and may be changed throughout their existence. The record of element origin and the changes tied to who made those changes is called provenance. Acquirers, integrators, and suppliers should maintain provenance of elements under their control to understand where the elements have been and who might have had an opportunity to change them.

Provenance is used when ascertaining the source of goods such as computer hardware to assess if they are genuine or counterfeit. Provenance allows for all changes from the baselines of components, component processes, information, systems, organizations, and organizational processes, to be reported to specific actors, functions, locales, or activities. Creating and maintaining provenance within the supply chain helps achieve greater traceability and is critical for understanding and mitigating risks. Doing so requires a process by which all changes to objects and activities within a supply chain and the persons, organizations, or processes responsible for authorizing and performing such changes are inventoried, monitored, recorded, and reported.

Provenance can be achieved through both physical and logical techniques, such as Configuration Management (CM), for tracking changes to the elements documenting the individuals who approved and executed these changes; robust identity management and access control to establish and record authorized or unauthorized activities or behaviors; and identification/tagging of elements, processes, roles, organizations, data, and tools.

#### **4.3.1 Acquirer – Programmatic Activities**

- a) Establish policies requiring the provenance of tools, data, and processes used throughout the system or element life cycle.
- b) Establish policies and procedures for tracking who has access and makes changes to individual elements and element processes throughout the supply chain.
- c) Establish policies to further stipulate that information related to the provenance of tools, data, and processes should be collected, processed, stored, and

disseminated in a controlled and protected manner equal to or greater than the individual items for which provenance is maintained.

- d) Establish policies to allocate responsibilities for review and approval of all changes in items subject to CM control.
- e) Ensure that all change control requirements are proposed, evaluated, and justified for their impact on elements, processes, systems, missions, and exposure to supplier or supply chain risks.
- f) Ensure that the organization develops, documents, and maintains under configuration control a current baseline configuration of elements, systems, and processes (both personnel and organizational), including communications- and connectivity-related aspects.
- g) Incorporate supply chain mitigations and practices into existing organization CM policies and procedures.
- h) Ensure that audit mechanisms are in place to track all changes upon approval.

#### **4.3.2 Integrators – General Requirements**

- a) Establish formally documented roles, responsibilities, and procedures to include the management information and documentation for establishing provenance.
- b) Establish policies and procedures for tracking who has access and makes changes to individual elements and element processes throughout the supply chain.
- c) Include requirements for the creation and tracking of the provenance of tools, data, and processes used throughout the system or element life cycle.
- d) Document the allocation of responsibilities for the creation, maintenance, and monitoring of provenance. Subject these records to internal controls and independent audit. Require protection of such records at a level commensurate with or greater than the protection of the items, processes, or activities they describe.
- e) Information in the CM system should be authenticated and non-repudiateable (digital signatures can be used to confirm this information).
- f) Record in CM system all changes to the element or system by processes initiated by either humans or automated systems.
- g) For system, element, process, and configuration changes, where change in element or process cannot be reversed or where non-repudiation of change is not possible, use a two-person rule for changes.
- h) Employ automated mechanisms and repeatable processes to address the number and frequency of changes and to minimize human interaction to minimize error. Ensure the timely collection of change throughout the system or element life cycle.
- i) Require the establishment and implementation of a policy to document, monitor, and maintain valid baselines for systems and elements, including spare parts and warehoused systems/elements, throughout the life cycle. Document changes to baselines and disseminate updated baselines to appropriate supply chain participants.
- j) Define, document, approve, and enforce physical and logical access restrictions associated with changes to the elements, systems, and processes.

- k) Protect information systems containing CM information against unauthorized exposure and access, including via physical and logical attacks.
- l) Create and implement a process for the CM of documentation, COTS or GOTS elements, and custom systems/elements. Perform security assessments of the CM processes and systems to attempt the detection of ongoing attacks (including the CM systems).
- m) Add new elements into the CM system as configuration items (CIs) when they are introduced into the supply chain.
- n) Ensure that audit mechanisms are in place to track all actual changes upon change control approval. Establish a verification process to provide additional assurance that the process of recording provenance and configuration change is working effectively, and that changes outside of these processes are technically infeasible or procedurally prohibited.
- o) For physical product delivery, maintain documentation of individuals who were in possession of an element at any time during purchasing, shipping, receiving, or transfer activities, including records of reviewer signatures for comparison.

#### **4.3.3 Suppliers – General Requirements**

- a) Provide documentation of formal processes for documenting roles, responsibilities, and procedures to include the management information and documentation for establishing provenance.
- b) Provide documentation on element baselines and maintenance throughout the system or element life cycle, including as part of logistics. Establish and implement a policy to monitor and maintain a valid baseline. Identify and implement appropriate levels of confidentiality, integrity, and availability including spare parts and warehoused systems/elements.
- c) Ensure information in the provenance and CM system is authenticated and cannot be repudiated (digital signatures can be used to confirm this information).

#### **4.3.4 Integrators – Technical Implementation Requirements**

- a) Document the use of mechanisms (tools and techniques) to assist in developing and maintaining the provenance of tools, data, and processes used throughout the system or element life cycle, including but not limited to use of CM or Configuration Control systems.
- b) Design and implement a two-person rule for system/element/process and configuration changes, where change in an element or process cannot be reversed, or where non-repudiation of change is not possible. Identify, document, and review any exceptions from the mandatory configuration settings for individual elements, systems, and processes based on the development, operational, and delivery requirements.
- c) Employ automated mechanisms, both centrally and through a trusted distributed CM system, whereby configuration settings are applied, managed and verified. (Note: Most automated CM systems work in both central and

distributed manner and can be set up to have a trusted distributed CM environment.)

- d) Incorporate detection mechanisms for unauthorized, security-relevant configuration changes into the organizations' incident response capability to ensure that detected CM events associated with element changes are tracked, monitored, corrected, and available for historical purposes.
- e) Ensure that backup 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.
- f) 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).
- g) Record location information of the actor making the change and where location information can be reliably obtained. Locations may be physical (e.g., geospatial) or logical (Internet Protocol [IP] address).
- h) Establish performance and sub-element baselines for the system and system elements. This helps detect unauthorized tampering/modification during repairs/refurbishing or unauthorized use of audit mechanisms. For example, consider using Radio Frequency (RF) interrogation of Integrated Circuits (ICs), and compare those results to results from known and trusted ICs.

#### **4.3.5 Suppliers – Technical Implementation Requirements**

- a) Establish configuration baselines for elements. This helps detect unauthorized tampering/modification during repairs/refurbishing or unauthorized use of audit mechanisms. For example, consider using RF interrogation of ICs, and compare those results to results from known trusted ICs.
- b) Document evidence that identity management and access control provide transparency into supplier personnel use of the CM system.

#### **4.3.6 Acquirer – Validation and Verification Activities**

- a) Verify the implementation and protection of systems of records used to create and maintain the provenance of data, tools, and processes based on security measures drawn from information security, physical security, industrial security, operations security, and IA.
- b) Document and test that the element, system, and processes (including modifications to the baseline configuration) conform to security configuration guidance – both to be deployed and or already deployed.

- c) Assess and test security measures to protect the provenance process, documentation, and system of records proposed by the security and system engineering communities.
- d) Review integrators' CM processes and activities, including monitoring and auditing of the CM systems to attempt detection of ongoing attack and if separate, completion of security assessments of the CM processes and CM systems.
- e) Audit integrators' ability to trace critical elements and processes throughout the supply chain.
- f) Audit integrators' ability to trace any authorized and unauthorized modifications to critical elements and processes throughout the supply chain.

#### **4.3.7 Integrators – Validation and Verification Requirements**

- a) Monitor and audit the CM systems to attempt detection of ongoing attacks.
- b) Perform security assessments of the CM processes and CM systems.
- c) Assess and test security measures to protect the provenance process, documentation, and system of records proposed by the security and system engineering communities.

#### **4.3.8 Suppliers – Validation and Verification Requirements**

- a) Demonstrate effective implementation of provenance processes and activities as well as CM mechanisms.
- b) Document the periodic assessment and testing of security measures to protect the provenance process, documentation, and system of records proposed by the security and system engineering communities.
- c) Provide documentation for the methods used for countering subversion and the loss of provenance, for example, backups, immutable chains in the CM mechanism (e.g., digital signatures proving a sequence of events), or recovery processes when subversion of a CM repository is detected.

### **4.4 Share Information within Strict Limits**

Acquirers, integrators, and suppliers need to share data and information. For the purposes of ICT SCRM, information sharing is the process by which acquirers, integrators, and suppliers (including COTS) exchange applicable data and information. The data and information that may be shared spans the entire system or element life cycle and the entire supply chain. Content to be shared may include data and information about the use of elements, users, acquirer, integrator, or supplier organizations, as well as information regarding issues that have been identified or raised regarding specific elements. Information that is sharable includes:

- Element design, development, test, evaluation, manufacturing, packaging for use, packaging for delivery, delivery processes, field sustainment, and depot sustainment;
- The threat agents, as well as the tactics, techniques, procedures, and tools used by threat agents to attack suppliers or elements;

- Past history of element and supplier performance as well as supplier track record in successfully resolving identified issues; and
- Agreements language including contract clauses, acquisition strategies, and construction of interagency agreements.

Information sharing is difficult to bind as the activity of sharing can be one-to-one, one-to-many, and many-to-many. The challenge for ICT SCRM is to ensure that information reaches specified individuals and organizations in quantity, quality, and with timeliness to perform required tasks or execute necessary functions.

Information sharing ultimately depends of the combination of attributes including the content of the information, the confidence in individuals, organizations, systems, and their defined roles and authorities. A combination of these attributes is needed in order to implement information-sharing techniques.

#### **4.4.1 Acquirer - Programmatic Activities**

- a) Define a policy that informs the supply chain about the sharing of information from the beginning to the end of the acquisition process. Include the following topics:
  - a. Which information is to be shared and which information is to be withheld from sharing;
  - b. Those individuals and organizations eligible to receive, store, use, and retransmit information;
  - c. The duration of information-sharing activities, as well as the events on which information sharing will begin and will be terminated;
  - d. Standards and requirements for protection of data at rest and in motion;
  - e. Standards to be used to protect shared information against unauthorized disclosure, access, modification, dissemination, or destruction, and unauthorized use of data and information;
  - f. Requirements for establishing identity of participants in information-sharing arrangements;
  - g. The means by which information sharing is executed and the mechanisms used to provide protection of information commensurate with the importance of such information; and
  - h. The planning and execution of audits of information-sharing activities.
- b) Enable selected authorized users to determine whether access authorizations assigned to sharing partners match the access restrictions on the information.
- c) Check incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination.
- d) Validate the binding of the information-sharing party's identity to the information at the transfer/release point prior to release/transfer from one domain to another.
- e) Protect requirements and supporting documentation from exposure or access that could result in the compromise or loss the confidentiality, integrity, or availability of the requirements.
- f) Develop source-selection criteria and procedures that encourage integrators and suppliers to provide acquirers visibility into elements, services, and processes as part of their contracts.

- g) Develop approaches that encourage integrators and suppliers to gain visibility into their supply chains as deeply as possible and reasonably. (1) Develop incentives that reward integrators for providing program-specific detailed technical information and technical data on products and services throughout the life cycle; and (2) include requirements that address the selection of open source elements.
- h) 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 the supply chain, technology, and risk to the system and elements throughout the life cycle, such as changes in suppliers, locations, process, and technology.
- i) Encourage integrators to provide technical details – both depth and breadth – about the 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.
- j) Encourage integrators to evaluate, document, and share element/element process information (including open source) that could result in weaknesses or vulnerabilities and if exploited, could result in loss or compromise.
- k) Define criteria for sharing types of evidence including: measures, activities, behaviors, and test results. Criteria may include conformance with specifications and standards, compliance with statutory or regulatory requirements, and compliance with contract terms and conceptions.
- l) 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. Please note that information published in errata may have vulnerability implications and thus should be screened before publishing.
- m) 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.
- n) 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.
- o) Based on the risk requirements of the mission and organization, consider using a centralized intermediary to acquire elements.
- p) Centralize support and maintenance services to minimize direct interactions that may expose confidentiality of system uses.
- q) 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, make the supply route less predictable through dynamic sourcing from multiple trusted suppliers.
- r) Prefer integrators and suppliers who can support centralized and/or dispersed buying approaches upon request.
- s) Share acquisition strategy and contract document approaches and language with other activities using or interested in common elements or suppliers.
- t) Where appropriate, devise contract requirements that can be reused by other projects, and encourage the use of common requirements.

- u) Provide an agreed-upon set of information security procedures to be used for information sharing across the element and system with various stakeholder communities (e.g., systems engineering, security, threat assessment, and threat response).

#### 4.4.2 Integrators - General Requirements

- a) Document all information-sharing arrangements in contract documents including:
  - a. Description of the information to be shared;
  - b. The conditions under which such information will be provided to recipients;
  - c. The terms and conditions governing the purposes and uses to which the shared information may be applied;
  - d. Standards for the protection of shared information against unauthorized disclosure or uses;
  - e. Standards and requirements for the protection of information at rest and in motion;
  - f. Mechanisms by which the identity of participants in information-sharing arrangements will be established;
  - g. Mechanisms and methods by which the required level of information protection will be achieved;
  - h. Responsibilities for monitoring and oversight of information-sharing practices, procedures, techniques, and mechanisms allocated; and
  - i. Assignment of planning and execution of information sharing and information protection audits.
- b) Separately document the instantiation of the techniques, procedures, and tools used to implement information-sharing agreements, and include the identity of participants in information-sharing activities, the means by which information sharing is executed, the mechanisms used to provide protection of information, commensurate with the importance or sensitivity of the information being shared and the planned and executed audits of information-sharing activities.
- c) Identify essential elements of information associated with each supply chain activity or task and the roles, processes, or organizations for whom access to such elements of information is necessary and sufficient to the successful performance of the supply chain. Such supply chain tasks could include, but are not limited to, requirements definition, acquisition and procurement planning, supply chain element creation, manufacturing, testing and evaluation, packaging for use, packaging for delivery, operational use, field and depot sustainment, and disposal and final disposition activities.
- d) Identify and assess alternative mechanisms, techniques, and procedures that could be used to facilitate the sharing of information necessary and sufficient to complete supply chain tasks. Such mechanisms could include manual, semi-automated, or fully automated systems and processes.
- e) Identify tactics, techniques, procedures, and tools that could be employed to protect information-sharing mechanisms and processes against unauthorized access or unauthorized use of information included in information sharing activities and processes.

- f) Apply identity management, access controls, and CM to the information-sharing activities and processes.
- g) Provide information sharing of audits from various communities (systems engineering, security, threat assessment, and threat response) for further assessment, evaluation, and response.
- h) Report to stakeholders the results of the review and assessment of negotiated changes in operational and technical requirements, technical specifications, and mandatory business practices.
- i) Prefer suppliers who maintain transparency about themselves, their elements, and their suppliers. For example, select suppliers who proactively provide:
  - a. Measures of continuous improvement in the usage of quality processes ISO/IEC 9001, ISO/IEC 27001, ISO 28000, and other certifications which can be leveraged to help ascertain existence of responsible quality practices as they pertain to SCRM; and
  - b. Measures such as Common Vulnerability Scoring System (CVSS) scores for vulnerabilities and fixes above a particular severity level, before the product ships.
- j) Protect against disclosing the uses of system, elements, or processes by which elements are designed, developed, produced, tested, delivered, or supported, or convey technological or operational advantage.
- k) Report supply chain threats and incidents in operational environments to agreed-upon recipient within established time frame parameters.
- l) Train system administrators and users regarding what information should be kept secure (for confidentiality, integrity, and availability) including not revealing supplier intermediaries.

#### **4.4.3 Suppliers - General Requirements**

- a) Document applicable information-sharing arrangements in contract documents including:
  - a. Description of the information to be shared;
  - b. The conditions under which such information will be provided to recipients;
  - c. The terms and conditions governing the purposes and uses to which the shared information may be applied;
  - d. Standards for the protection of shared information against unauthorized disclosure or uses;
  - e. Standards and requirements for protection of information at rest and in motion;
  - f. Mechanisms by which the identity of participants in information-sharing arrangements will be established;
  - g. Mechanisms and methods by which the required level of information protection will be achieved;
  - h. Responsibilities for monitoring and oversight of information-sharing practices, procedures, techniques, and mechanisms allocated; and

- i. Assignment of planning and execution of information sharing and information protection audits.
- b) Separately document the instantiation of the techniques, procedures, and tools used to implement information-sharing agreements, and include the identity of participants in information-sharing activities, the means by which information sharing is executed, the mechanisms used to provide protection of information commensurate with the importance of or sensitivity of the information being shared, and the planned and executed audits of information-sharing activities.
- c) Document various tactics, techniques, procedures, and tools that could be employed to protect information-sharing mechanisms and processes against unauthorized access or unauthorized use of information included in information-sharing activities and processes.

#### **4.4.4 Integrators - Technical Implementation Requirements**

- a) Implement information-sharing tasks by identifying essential elements of information to be shared as required for the completion of activities such as requirements definition, acquisition and procurement planning, supply chain element creation, manufacturing, T&E, packaging for use, packaging for delivery, operational use, field and depot sustainment, and disposal and final disposition.
- b) Identify mechanisms, techniques, and procedures that can be used to facilitate the sharing of information and match them with the content, data type, and data volume to be shared so that:
  - a. Only the information necessary and sufficient to complete supply chain tasks is shared; and
  - b. Information sharing can be used to identify and further protect elements and information that, if disclosed or accessed, could compromise the confidentiality, integrity, or availability of supply chain elements, processes, or actors within the supply chain.
- c) Define technical specifications and measures derived from operational requirements to protect supply chain processes 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 of confidentiality, integrity, or availability.
- d) Apply identity management, access controls, and CM to the requirements process to ensure the confidentiality, integrity, and availability of requirements and supporting data, information, and requirements development tools.
- e) Encourage suppliers to provide technical details about their elements and/or services where appropriate. Examples of information may include interface specifications, configuration details, element processes, and any known weaknesses and vulnerabilities. Such information may be important to enable follow-on support, including when an element or service is no longer available.
- f) Limit disclosure of delivery process information.
- g) Configure systems and elements, as well as items delivered as part of support and maintenance activities, to conceal the uses of the system/element (e.g., disable or redirect “phone home” functions).

- h) Limit disclosure of testing methods and procedures, test data, and communication routes by which such data is distributed, analyzed, and reported.

#### **4.4.5 Suppliers - Technical Implementation Requirements**

- a) Identify mechanisms, techniques, and procedures that can be used to facilitate the sharing of information and match them with the content, data type, and data volume to be shared such that information sharing:
  - a. Allows only the information necessary and sufficient to complete supply chain tasks; and
  - b. Can be used to identify and further protect elements of information that, if disclosed or accessed, could compromise the confidentiality, integrity, or availability of supply chain elements, processes, or actors within the supply chain.
- b) Document technical specifications and measures to protect supply chain processes 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 of confidentiality, integrity, or availability.
- c) Limit disclosure of delivery process information.
- d) Configure the element for delivery to conceal the uses of the element (e.g., disable or redirect “phone home” functions).
- e) Limit disclosure of testing methods and procedures, test data, and communication routes by which such data is distributed, analyzed, and reported.

#### **4.4.6 Acquirer - Validation and Verification Activities**

- a) Assess the implementation of protection mechanisms regarding information-sharing activities through the development of combinations of information security, IA, physical security, personnel security, and operations security activities.
- b) Audit results of implemented filters that constrain data structures and content to information security policy requirements when transferring information between different content or security domains
- c) Verify and document the implementation of identity management, access controls, and CM to information-sharing activities and the confidentiality, integrity, and availability data and information being included in such activities.
- d) Evaluate the processes by which information is shared in response to the compromise or loss of confidentiality, integrity, and availability of information, supply chain elements, or supply chain processes.

#### **4.4.7 Integrators - Validation and Verification Requirements**

- a) Assess the implementation of information-sharing activities through the development of combinations of information security, IA, physical security, personnel security, and operations security activities.
- b) Audit the effectiveness of information-sharing policies and their implementation.
- c) Monitor the information flows and interrupt the unauthorized exchange of information when such exchanges are attempted.
- d) Verify the implementation of identity management, access controls, and information-sharing activities to the confidentiality, integrity, and availability data and information being included in such activities.
- e) Perform assessments to measure the risk to the supply chain posed by information-sharing activities including the people, organizations, information sharing-processes, and systems.
- f) Verify that all supply chain participants are sharing information in response to compromise or loss of confidentiality, integrity, and availability of information, supply chain elements, or supply chain processes.
- g) Verify that information is shared on proposed measures that could be employed to prevent exposure of or access to information on elements, processes, and suppliers in the event that proposed supply chain changes are adopted.
- h) Employ operational security tactics, techniques, and procedures to verify that access to information shared with potential integrators and suppliers sustains and enhances the confidentiality of element uses.

#### **4.4.8 Suppliers - Validation and Verification Requirements**

- a) Document the assessment and implementation of protection mechanisms regarding information-sharing activities by establishing combinations of information security, IA, physical security, personnel security, and operations security activities.
- b) Audit the effectiveness of information-sharing policies and their implementation.
- c) Verify and document the implementation of identity management, access controls, and CM to information-sharing activities and the confidentiality, integrity, and availability data and information being included in such activities.
- d) Document the processes for sharing information in response to the compromise or loss of confidentiality, integrity, and availability of information, supply chain elements, or supply chain processes.

### **4.5 Perform Supply Chain Risk Management Awareness and Training**

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. Additionally, the ISO/IEC 27001 information security management standard and the ISO 28000:2007 supply chain process integration and certification standard provide an organization-wide program that includes training. This practice focuses on supply chain-specific awareness and training practices. In general, the training should include all applicable practices found in this document.

#### **4.5.1 Acquirer Programmatic Activities**

- a) Establish organizational policy and general contractual requirements that address personnel SCRM awareness and training throughout acquirer and integrator organizations.
- b) Develop a comprehensive awareness and training program that promotes the organization's SCRM policy and procedures.
- c) Require SCRM awareness training for all acquirer and integrator personnel involved in requirements, acquisition, and procurement activities.
- d) Train acquirer personnel to evaluate integrators based on past performance related to personnel policies, procedures, and security practices as part of source selection requirements and processes.
- e) Define processes by which general supply chain information and lessons learned will be collected and shared between acquirers, integrators, and suppliers as scoped within the contract.
- f) Provide training to appropriate acquirer staff on standard commercial approaches for acquiring secondary market (refurbished) items, to ensure that secondary market items are adequately supported and maintained.

#### **4.5.2 Integrator – General Requirements**

- a) Conduct SCRM awareness and training for key personnel to include identifying deficits/weaknesses and faults/vulnerabilities in the supply chain and appropriate mitigation actions. If appropriate, incorporate into existing training on business risk - such as protection of intellectual property. (Training may also be part of a variety of certification processes including the ISO 28000:2007 supply chain certification process or the ISO/IEC 27001 information security management system certification process.)
- 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. This includes changes of roles and personnel associated with transitioning a system to an organization operating the system and any associated suppliers.
- c) Provide training to appropriate integrator staff on standard commercial approaches for acquiring secondary market (refurbished) items, to ensure that secondary market items are adequately supported and maintained.

### **4.5.3 Supplier – General Requirements**

- a) Conduct SCRM awareness and training for supplier personnel to include identifying deficits/weaknesses and faults/vulnerabilities in the supply chain and appropriate mitigation actions. If appropriate, this training should be incorporated into existing training on business risk, such as the training addressing protection of intellectual property. (Training may also be part of a variety of certification processes including the ISO 28000:2007 supply chain certification process or the ISO/IEC 27001 information security management system certification process.)
- b) Document the existence of training of appropriate supplier staff on standard commercial practices for acquiring secondary market (refurbished) items, to ensure that secondary market items are adequately supported and maintained.

### **4.5.4 Integrator – Technical Implementation Requirements**

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

### **4.5.5 Supplier – 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 receiving elements/services (including spare parts), including any known anomalies in parts (which may indicate counterfeits, subversion, or quality issues).

### **4.5.6 Acquirer - Validation and Verification Activities**

- a) Monitor and review contract documents to ensure that requirements for awareness and training are included and are adequate.
- b) Review integrator performance of supply chain risk awareness and training against requirements.
- c) Assess integrator effectiveness of supply chain risk awareness and training.

### **4.5.7 Integrator - Validation and Verification Requirements**

- a) Evaluate awareness and training program for effectiveness at ensuring that personnel understand supply chain threats and are exhibiting appropriate behavior to address them.
- b) Provide periodic documentation demonstrating the implementation and operation of a comprehensive SCRM training program.
- c) Provide periodic updates on the status of personnel SCRM training in support of contractual requirements.

#### **4.5.8 Supplier - Validation and Verification Requirements**

- a) Demonstrate the implementation and operation of SCRM training and awareness program within the supplier organization.

### **4.6 Use Defensive Design for Systems, Elements, and Processes**

The use of design concepts is a common approach to delivering robustness in security, quality, safety, diversity, and many other disciplines that can aid in achieving ICT supply chain assurance. Defensive design techniques should be applied to supply chain elements, element processes, information, systems, and organizational processes throughout the system or element life cycle. Element processes include creation, testing, manufacturing, delivery, and sustainment of the element throughout its life. Organizational and business processes include issuing requirements for acquiring, supplying, and using supply chain elements.

Defensive design techniques explicitly address contingencies in the technical, behavioral, and organizational activities that could result in adverse supply chain events. Defensive design is intended to create options that preserve the integrity of the mission function and its performance to the end user or consumer of the supply chain element should any of the contingencies or contingency elements arise. Defensive design provides flexibility to handle uncertainty and the ability to adapt to changing circumstances including environmental, malicious, or unintentional harm within the supply chain.

Element and supply chain defensive design can increase robustness against attack by reducing the likelihood or consequences of attack. Defensive design techniques include activities that consider and test supply chain elements, element processes, and organizational processes for potential failure modes and the compromise or loss of confidentiality, integrity, or availability of information. For example, during the development of requirements, defensive design considerations can explore the consequences of compromising identity. During later phases of the system or element life cycle, defensive design considerations can examine the potential consequences of compromise or loss of test data integrity, and devise a set of alternative tests or delivery processes that would offset the loss of test data confidentiality. Defensive design can also help to ensure availability of required elements and continued supply in the event of compromise to the system/element.

Defensive design can help reduce the impact of an attack on ubiquitous elements if more than one type of element is used (e.g., routers from multiple manufacturers). Of course, this has to be balanced with economies of scale to manage maintenance and support costs. Defensive design also includes the review of chosen elements for achieving diversity, uses of a new design element, and a range of alternative features that could be promulgated should the compromise or loss of confidentiality be suspected or detected, providing a feedback loop for continuous improvement of supply chain elements and element processes.

#### 4.6.1 Acquirer – Programmatic Activities

- a) Define, design, and implement roles for individuals, organizations, elements, and element processes throughout the system or element life cycle to limit or constrain:
  - a. Unmonitored or uncontrolled activity across multiple elements, processes, organizations, or systems;
  - b. The opportunities or means for unauthorized exposure that can lead to the compromise of elements, element processes, systems, or information; and
  - c. The inability to detect or monitor adverse events.
- b) 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.
- c) Review and evaluate the system/element criteria and requirements for diversity.
- d) Develop contract documents that require the use of widely used and/or international standards where practical and feasible to increase potential diversity of supply channels. Standards promote interoperability (i.e., protocols) and thus aid in the possibility that a replacement may be manageable. This may be more easily applied in the case of commodity software or hardware.
- e) Develop organizational policies and procedures that consider an assessment of potential supply chain risks prior to making decisions restricting or limiting diversity of elements or suppliers.
  - a. Such assessments should discuss the pros and cons of the exposure of elements, supplier/integrator vulnerabilities, and opportunities for exploitation based on known adversarial tactics, techniques, procedures, or tools (for example, so that they could be mitigated through diversifying elements or the supply chain).
  - b. Identify cases where a standard configuration may reduce costs, but could increase risks due to known adversary tactics, techniques, and procedures.
- f) 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.
- g) Require integrators and suppliers to deliver elements and element processes with the most advanced security configurations and designs to limit access and exposure.
- h) Develop a comprehensive testing policy and procedures.
- i) Require that the system's operational environment protect the system both physically and logically. Include applicable system integration and custom code extension activities as part of the upgrade and maintenance efforts in system operation requirements.
- j) Develop and implement an approach for handling and processing reported supply chain anomalies. Require the separation of duties for people and

organizations as well as the separation of functions for supply chain elements and element processes.

- k) Require redundancy and diversity throughout the supply chain and document the benefits, risks, and contingency plans to respond to supply chain risks resulting in decisions to reduce diversity and redundancy or alternatives in availability of supply chain elements or element processes.
- l) Use threat assessment techniques and information to determine if the proposed design alternatives meet defensive design criteria.
- m) Use threat analysis techniques (such as threat modeling) to examine the element's design vulnerabilities.
- n) Model, simulate, test, and evaluate the supply chain risks prior to decisions to limit the diversity of system/elements or suppliers.
- o) Avoid use of counterfeit/grey market elements as much as possible. Define and document processes for making decisions regarding keeping or disposing of counterfeit/grey market elements for when no other appropriate sources of supply can be found or for those cases when counterfeit/grey market elements are found already in the supply chain. Should a decision be made to keep or use grey market elements, after careful consideration, define and document the processes for how to procure, integrate, and maintain them.

#### **4.6.2 Integrators – General Requirements**

- 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) Define and implement processes by which elements are selected for use in systems. Specify use of genuine and tested elements.
- c) Define the system/element requirements to allow for diversity in element supply.
- d) 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. 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.
- e) Define and/or use standards-based technical interfaces and process requirements to provide options for the modification of processes or modification/replacement of elements should a supply chain compromise occur.
- f) 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/grey market elements or product intrusions.
- g) Establish an adequate supply of trusted spare and maintenance parts for use well beyond the life span of the element.
- h) For critical elements/services, determine the specific source of the element/service, not merely a corporate or organizational identity.

- i) 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.
- j) For critical elements, consider using preapproved sources (e.g., trusted foundry/trusted integrated circuits for elements containing integrated circuits).
- k) Conduct an assessment of potential supply chain risks prior to making decisions restricting or limiting diversity of elements or suppliers, including legacy suppliers. Assessments should:
  - a. 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;
  - b. Identify cases where a standard configuration may reduce costs, but can increase risks due to known adversarial tactics, techniques, and procedures; and
  - c. Document risk-based decisions, taking above concerns into consideration.
- l) Consider using more than one implementation or configuration of both the supply chain and the system/element.
- m) For critical infrastructure systems, 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.
- n) Ensure that elements are assigned varying degrees of criticality depending on the purpose and use of each element.
- o) Ensure the continued availability of required elements and continued supply in the event of compromise to the system/element through diversity of supply (especially on commodity functions).
- p) Ensure the removal or the turning off of any unnecessary functions that are prevalent in COTS or in some cases, GOTS. This would include implementations that may be designed to support multiple applications or purposes. If left active, these functions may permit unauthorized access or exposure of the system or perform a function that reduces the availability of other functions.
- q) Prefer elements that use widely used and/or international standards, making it more feasible to replace them.
- r) Implement and maintain mechanisms to deliver appropriate privileges, separation of duties, provenance, 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.
- s) 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.)
- t) Use two-person control when performing custom development and integration of critical elements and performing critical processes, such as paired development processes.

- u) When counterfeit/ grey market elements are found in the supply chain, notify the acquirer immediately. Work with the acquirer to decide whether to keep or dispose of these elements, and should a decision be made to use them, how to integrate them.
- v) 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.

#### **4.6.3 Suppliers – General Requirements**

- a) Document the uses of processes by which elements are selected for use in systems. Specify the use of genuine and tested elements.
- b) Report to the acquirer any element vulnerabilities including those exposed by element maintenance changes, standard interface changes, patches, and upgrades. Leverage industry best practice for security patches to include a list of what issues are “covered” in the patches (i.e., the nature of the issues, a severity rating such as CVSS, etc.).
- c) Deliver, where appropriate, sufficiently robust elements that do not degrade in performance, even when out-of-bounds inputs are provided (where practicable).
- d) 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.
- e) Establish manual review as a practice, to be employed as appropriate into the system or element life cycle, to identify and remediate any weaknesses and vulnerabilities; include peer reviews (e.g., walk-throughs and inspections) and comprehensive or sampled reviews.
- f) Establish processes that address code changes that are authorized, validated, and tested (to ensure they do not introduce regressions or break other functionality). Apply fuzz testing or static analysis to assess robustness of code and aid in identification of defects.
- g) Establish processes to identify individual products and notify the acquirer when open/counterfeit/ grey market products are mixed with products from authorized distribution or OEMs.
- h) Document the use of processes that limit entrance of counterfeit/ grey market items into the supply chain and when entered/breached, the processes for corrective action.

#### **4.6.4 Integrators – Technical Implementation Requirements**

- a) Use existing resources such as market/technical analysis results, prequalified product lists (e.g., available from General Services Administration (GSA), DHS, or internal integrator list) for identifying candidate elements. If applicable, require elements to have certifications and validations such as Common Criteria, FIPS 140-2 validation, and Federal Desktop Core

Configuration (FDCC)/ United States Government Configuration Baseline (USGCB).

- b) Consider using more than one implementation of the supply chain or more than one implementation or configuration of the element.
- c) Consider using paired development/manufacturing for systems and elements as it provides checks and balances for both intentional and unintentional insertions of malware and also provides a way to monitor the quality of development/manufacturing.
- d) Identify and document diversity of suppliers to facilitate a change if the original supplier becomes unavailable.
- e) Review elements to determine if source information matches are found on the approved products lists, and whether ownership has changed since its approval.
- f) Consider placing elements in escrow and not (fully) paying for those elements until verification of authenticity and acceptance testing of element is complete.
- g) If counterfeit/ grey market items have entered the supply chain, take actions to reduce the potential for subversion including additional verification, searching for malware, verifying firmware patches, comparison with known good products, and establishing larger stockpiles of spares.
- h) Include protection for data at rest and in motion including, but not limited to, the use of various forms of encryption.
- i) Assess the design and implementation of identity management, access controls, and process monitoring mechanisms to facilitate timely detection and classification of anomalous behaviors that may result in adverse consequences through observation of tasks and activities.
- j) Use robust programming languages that do not have inherent security flaws for the development of operational requirements and technical specifications.
  - a. 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.
  - b. Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements.
- k) Use structured and standardized approaches to reduce the complexity of the design, production, and implementation of both the system and the environment.
- l) Identify and implement interface standards wherever practical to promote system and element sustainability and element reusability.
- m) Use industry best practices, such as Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), NSA SNAC (Systems and Network Analysis Center) guides, and NIST Special Publications and configuration checklists, to define secure configuration requirements and to configure elements to increase security and limit unnecessary functionality.

- n) Determine the acceptability of, and document the presence of, abused behaviors or design deficits or weaknesses that could become vulnerabilities if exploited (e.g., “call home” functionality, default passwords that do not require change before use).
- o) 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.
- p) 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).
- q) Limit the number, size, and privileges of critical elements.
- r) Design elements to withstand out-of-bounds inputs (e.g., excessive voltages, numbers out of range, and so on), so that they are harder to disable.
- s) Include fail-over/redundant systems or system elements when possible and appropriate.
- t) Use FIPS 140-2-validated cryptographic modules at rest and (in motion) and anti-tamper (including tamper-resistant and tamper-evident) mechanisms to counter theft and subversion (including auto-destruction if tampering is detected).
- u) 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.
- v) 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.
- w) Develop bounding cases for design or operation for both elements and element processes to identify potential compromise or loss of confidentiality, integrity, or availability that would impact cost, schedule, or performance of those elements and element processes, as well as missions that they support throughout each system or element life cycle phase.
  - a. Consider a broad range of contingencies (hazards) including natural events, unintentional actions by individuals or organizations, or intentional actions by individuals and organizations that might impact mission accomplishment.
  - b. Examine cases where the application of standard configurations may reduce costs but present an increased risk of mission failure or unauthorized exposure of, or access to, supply chain elements.
- x) 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.

- y) Use a variety of testing techniques including fuzz testing, static analysis testing, dynamic testing, and penetration testing to identify architecture, design, and implementation weaknesses, search for common security weaknesses and vulnerabilities, search for virus/malware signatures, identify failures to comply with standards and requirements including process requirements, and identify areas in need of in-depth testing.
  - a. Test for compliance on both ends of interfaces. The use of standardized interfaces may facilitate the expanded use of test suites and potentially increase the breadth of testing.
  - b. 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.
  - c. Use both negative and positive tests to verify that the system/element/process does not do what it should not do, as well as that it does what it is supposed to do.
  - d. Monitor for unexpected or undesirable behavior during testing, such as network behavior (e.g., a surprise “call home” or opening of network port), file system behavior (e.g., reading or writing information to unexpected files/directories), race conditions, and deadlocks.
  - e. Protect test cases and test results from unauthorized access by using encryption, signatures, and other methods. For example, for software, ensure that test cases and test results are signed to demonstrate absence of tampering.

#### **4.6.5 Suppliers – Technical Implementation Requirements**

- a) Document the presence of easily abused behaviors or design deficits or weaknesses that could become vulnerabilities if exploited in both elements and element processes.
- b) Document various defensive design techniques used on the logical and physical design, manufacturing, and supply chain environment.
- c) Document the variety of testing techniques used to verify whether the element can be trusted.
- d) Provide elements “secured by default” at a level appropriate to the requirements of the acquiring organization.
- e) Deliver elements in a manner that facilitates proof of authenticity verification by the acquirer.
- f) Provide configuration documents in human-readable text and Security Content Automation Protocol (SCAP)-consumable form that describes how to configure COTS elements to limit their functionality or increase their security, to avoid unnecessary or dangerous functionalities.

- g) Verify the use of both negative and positive tests to ascertain that the system/element/process does what it is supposed to do and does not do what it should not do.
- h) Monitor for unexpected or undesirable behavior during test, such as network behavior (e.g., a surprise “call home” or opening of network port), file system behavior (e.g., reading or writing information to unexpected files/directories), race conditions, and deadlocks.
- i) Establish a trusted baseline for the system and operational configuration based on service-level agreements (SLAs). Use this baseline to identify unauthorized changes or tampering.
- j) Use existing vulnerability and incident management capabilities to identify potential supply chain vulnerabilities.

#### **4.6.6 Acquirer – Validation and Verification Activities**

- a) Review integrators’ quality assurance processes to ensure compliance with requirements, Federal Procurement Policy, and FAR.
- b) Examine the element to ensure that it is as specified in requirements and that it is new, genuine, tested, and that all associated licenses (including support agreements) are valid.
- c) Assess proposed or implemented design, development, test, evaluation, assembly, manufacture, packaging, delivery, and sustainment processes for weaknesses (deficits) or faults (vulnerabilities) to determine their robustness and potential for compromise of confidentiality, integrity, or availability of elements and element processes, systems, information, and organizations. The results of such evaluations, assessments, and tests should be shared with the security community as well as systems engineers and other supply chain participants, in accordance with relevant information-sharing processes.
- d) Monitor, evaluate, test, and Red/Blue 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.
- e) Consider use of third parties to evaluate and test elements when those capabilities do not exist in-house.
- f) Perform audits of defensive design practice requirements throughout the system or element life cycle.
- g) Review test and evaluation results throughout the life cycle to ensure compliance with configuration requirements as defined within the program.
- h) Review and evaluate the application of criteria and decision outcomes for diversity choices against contractual requirements.
- i) If counterfeit/ grey 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.
- j) Monitor and audit systems and operations to reduce the risk of unauthorized removal, replacement, and/or modification of elements. Modification review

may include applicable system integration and custom code extension activities as part of the upgrade and maintenance efforts for system operations.

- k) Periodically audit integrator system activities for compliance with requirements/Service-Level Agreement (SLA) and to detect potential supply chain issues. This may include the review of any reports providing a summary of any detection of malicious functionality, known vulnerabilities, or changes in suppliers or supplier venue.
- l) Perform assessments of potential failure modes and effects on various proposed element designs based on the application of hypothesized or observed tactics, techniques, procedures, and tools of threat sources.
- m) Assess the effectiveness of alternative configurations in protecting the confidentiality, integrity, or availability of elements, processes, systems, and information against potential or observed threat sources.
- n) Design, develop and apply physical and industrial security, information security, and IA tactics, techniques, and procedures to support design, definition, and implementation of roles to reduce opportunities for adverse consequences.
- o) Assess the introduction of deficits, weaknesses, vulnerabilities, faults in, and opportunities for potential exposure of or access to elements or element processes as a result of different implementations of standards.

#### **4.6.7 Integrators – Validation and Verification Requirements**

- a) Examine the element to ensure that it is new, that it was specified in the requirements, and that all associated licenses are valid.
- b) Identify past vulnerabilities in elements and element processes to determine if they have been addressed and what they indicate about the strength of the elements' security.
- c) Implement a third-party assessment process for acceptance testing to ensure elements are genuine.
- d) Verify that the element's performance does not degrade or cause system failure even when out-of-bounds inputs are provided (where practicable).
- e) 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.
- f) Assess opportunities for the introduction of weaknesses and vulnerabilities in systems and elements as a result of different implementations of standards.
- g) Assess the proposed use of government or military standards to guard against the unnecessary exclusion of other standards that unduly restricts choices of potential elements or suppliers.
- h) Assess the effectiveness of alternative configurations in protecting the confidentiality, integrity, or availability of elements, processes, systems, and information against known vulnerabilities.
- i) 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. Include an assessment

- of testing results (from all types of testing) to identify additional vulnerabilities, and report results of such assessments.
- j) Model, simulate, test, and evaluate supply chain risks prior to decisions to limit the diversity of system/elements or suppliers.
  - k) 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.
  - l) For COTS, make integrator assessments of supplier technologies to the suppliers, when appropriate, to ensure transparency and promote technology improvements.

#### **4.6.8 Suppliers – Validation and Verification Requirements**

- a) Implement various system and organizational certification requirements to provide rigor in the process to demonstrate a quality assurance mechanism's facet of defensive design. A management system certification, such as ISO 9001, ISO/IEC 27001, or ISO 28000, may provide evidence of quality assurance, security, and supply chain management processes.
- 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 should consider time of use, information being used (e.g., directories), applications, equipment, and connections used.

### **4.7 Perform Continuous Integrator Review**

Continuous integrator review is a critical practice used to ascertain that defensive measures have been deployed. It includes testing, monitoring, auditing, assessments, and any other means by which the acquirer observes integrator and supplier practices. The purpose of continuous integrator review 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 the associated metadata.

The continuous integrator review will help determine if remedial actions are required based on the environment and use. Continuous integrator review should be conducted in multiple contexts including the selection of COTS elements, integrating COTS and GOTS into larger systems, and accepting the delivery of COTS, GOTS, custom, or open sources elements. This may be done at different points during the system or element life cycle including development, operations, sustainment, and disposal.

This practice focuses on the integrator rather than on the supplier. The relationship between the integrator and the acquirer requires a great deal of transparency and traceability as the integrator is more than likely providing a combination of service and product under an agreement. The integrator is likely to have access to acquirer's systems, facilities, people, and processes. The integrator is also likely to use their own

infrastructure to develop, integrate, or maintain the acquirer's systems. By definition, this relationship has a great number of dependencies including a substantial amount of information and data exchange. In contrast, the relationship between the acquirer and the supplier involves less collaboration to create custom solutions and sharing of information and infrastructure. Therefore, acquirers have a limited ability to review supplier processes.

However, integrators are encouraged to review their own relationships with individual suppliers and apply those practices as appropriate, especially in the case of suppliers being custom development houses.

#### **4.7.1 Acquirer – Programmatic Activities**

- a) Develop and implement a comprehensive integrator review policy and procedures that span the system or element life cycle and use multiple methods, including testing, monitoring, assessment, and auditing.
- b) Require, where applicable, periodic, independent third-party audits of integrator systems.
- c) Define specific types of continuous integrator review to be required in procurements.
- d) Examine the hiring and personnel policies and practices of integrators to assess the strengths or weaknesses of the personnel security policies and procedures.
- e) Require the review of operational and technical requirements and mandatory business practices (processes and rules). Include reviews 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. When requirements result in proposed changes in the supply chain, evaluate these changes for increased opportunities of adversary exposure of, or access to, elements, element processes, or supplier business processes.
- f) Evaluate changes in the supply chain environment or the context of system/element 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.
- g) Define criteria and thresholds for identifying and tracking critical elements that require modification or replacement throughout the supply chain. These thresholds should be set well before an element's expected retirement from service and based, for example, on mean-time-between-failures (MTBF) for hardware and the number of releases for software.
- h) Require the integrator to monitor supplier activities, as appropriate, to detect and assess threats or attempts to gain, or exploit exposure of, access to elements, supply chain processes, or supply chain actors.
- i) Require that reviewers are qualified to identify weaknesses and vulnerabilities in the supply chain or integrator SCRM processes and procedures.
- j) Continuously monitor acquirers' and integrators' internal controls over the allocation of tasks and activities to roles.

- k) Test acquirers' and integrators' internal controls for their effectiveness in detecting anomalous behavior and timely intervention to prevent or reduce adverse consequences.
- l) Assess the effectiveness of protective measures against threat sources' ability to gain access to the processes, system, or elements. Measures of protective effectiveness include time delay, required level of effort by the adversary, or ease of detection.
- m) Review personnel security policies and practices of all integrators.
- n) Require implementation of static and dynamic analysis for selected elements and processes (e.g., automated manufacturing/test processes and delivery mechanisms).
- o) Require that penetration testing be a realistic simulation of the active adversary's known adversary tactics, techniques, procedures, and tools. State the conditions and criteria throughout the life cycle for physical and logical penetration testing of systems, elements, or processes.
- p) When practical for evaluating potential critical system elements, prefer integrators and suppliers that have incorporated static and dynamic analysis as best practices into their system or element life cycle process before: 1) making a make-buy decision; 2) selecting COTS, GOTS, custom or open sources elements; and 3) accepting COTS, GOTS, custom or open sources elements into the system.

#### **4.7.2 Integrators – General Requirements**

- a) Continuously monitor internal controls in addressing the allocation of tasks and activities to roles.
- b) Test internal controls for their ability to detect anomalous behavior and facilitate timely intervention to prevent or reduce adverse consequences.
- c) Assess the effectiveness of protective measures against threat sources' to gain access to processes, systems, or elements. Measures of protective effectiveness include time delay, required level of effort by the adversary, or ease of detection.
- d) Perform manual reviews of the elements, processes, and systems 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.)
- e) Apply various testing and analysis tools to potential system elements before: 1) making a make-buy decision; 2) selecting COTS, GOTS, custom, or open-source elements; and 3) accepting COTS, GOTS, custom, or open-source elements into the system.
- f) Verify that processes addressing code change incorporation are authorized, validated, and tested (to ensure they do not introduce new vulnerabilities, regressions, or break other functionality).
- g) Determine the conditions and criteria throughout the life cycle for physical and logical testing of systems, elements, or processes.

- h) Identify and track critical processes and elements throughout the supply chain that require modification or replacement well before an element's expected retirement from service, based, for example, on MTBF for hardware and based on the number of releases for software.
- i) Determine and document hardware failure rates and periodically verify these rates.
- j) Determine and document critical numbers of software patches or the extent of releases that would leave software vulnerable.

#### **4.7.3 Suppliers – General Requirements**

- a) None

#### **4.7.4 Integrators – Technical Implementation Requirements**

- a) None

#### **4.7.5 Suppliers – Technical Implementation Requirements**

- a) None

#### **4.7.6 Acquirers – Validation and Verification**

- 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 the integrator's 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.
- c) Review the integrators' processes and procedures aimed at limiting exposure of system and elements uses.
- d) Ensure that the integrator assess known adversary tactics, techniques, and procedures; tools against physical, information security and IA; and personnel security practices employed to protect the supply chain environment.
- e) Perform/outsourcing acceptance testing to ensure compliance with performance specifications.
- f) Incorporate testing results (from all types of testing) into the oversight of other supply chain practices.
- g) Monitor and assess the implementation and results of manual review requirements to ensure compliance with laws, regulations, and policies as well as conformance to contract specifications or standards.
- h) Monitor and assess the implementation and results of applying various testing techniques (for example, penetration testing or baseline testing before accepting the system).

#### **4.7.7 Integrators – Validation and Verification Requirements**

- a) Monitor supplier activities, as appropriate, 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) Monitor and assess the implementation of systems and the results of manual review requirements to ensure compliance with laws, regulations, and policies, as well as to ensure conformance to contract specifications or standards.
- c) Assess testing results (from all types of testing) to identify additional vulnerabilities and report results of such assessments to the acquirer.
- d) Perform technical and procedural audits of mechanisms used to shield the uses of the element.

#### **4.7.8 Suppliers – Validation and Verification Requirements**

- a) None

### **4.8 Strengthen Delivery Mechanisms**

Delivery, including inventory management, is a critical function within the supply chain and has a great potential for being compromised. In today's ICT environment, delivery can be both physical (e.g., of hardware) and logical (e.g., software modules and patches). Delivery happens at any point across a system or element life cycle, among multiple parties and multiple links of a given supply chain, and includes acquirers, multiple integrators, and multiple suppliers.

Because delivery may be compromised anywhere along the supply chain and system or element life cycle, both physical and logical element delivery mechanisms should adequately protect the confidentiality, integrity, or availability of systems and elements delivered through the supply chain. This practice addresses the steps needed to strengthen the delivery mechanisms to ensure that opportunities are not provided for unauthorized access or exposure to the element, processes and system, as well as information about their uses, which can result in unauthorized modification (including substitution and subversion) or redirection by active adversaries to an alternate location.

#### **4.8.1 Acquirer – Programmatic Activities**

- a) Require that systems and elements are incorporated into the organization's inventory management system.
- b) Examine organization's inventory management policies and processes to ensure that they include:
  - a. How to request replacements;
  - b. Appropriate stocking, including the location and protection of spares;
  - c. Receipt policies to define who the inventory should go to, when it arrived, who handled it, where it is located, and if the received inventory is reconciled to what was ordered; and

- d. Inventory counting and accounting policies.
- c) Determine which 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 personnel inventory management policies and processes.
- e) Maintain a level of physical and/or logical access control (i.e., locking file cabinets on the integrator premises), where relevant, for all purchase order/delivery authorizations for physical product delivery.

#### **4.8.2 Integrators – General Requirements**

- a) Establish processes to assure that the system or element will to be delivered when they are needed:
  - a. Modify the delivery path so that it is difficult to prevent delivery (e.g., via sabotage); and
  - b. Define multiple vetted delivery paths, in case a delivery path is unavailable or compromised.
- b) Establish minimum baselines for supply chain delivery, processes, and mechanisms.
- c) 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 and element while storing before use (including spares).
- d) Design delivery mechanisms to avoid exposure or access to the system and element delivery processes, and use of the element during the delivery process.
- e) Implement delivery processes for the intended logical and physical transfer and receipt of elements to be done by authorized personnel.
- f) Require education and training for personnel inventory management policies and processes.
- g) Use nondestructive techniques or mechanisms to determine if there is any unauthorized access throughout the physical delivery process.
- h) Maintain a level of physical and/or logical access control (i.e., locking file cabinets on the integrator premises), where relevant, for all purchase order/delivery authorizations for physical product delivery.

#### **4.8.3 Suppliers - General Requirements**

- a) Establish processes to ensure that the system or element will be delivered when they are needed:
  - a. Modify the delivery path so that it is difficult to prevent delivery (e.g., via sabotage); and
  - b. Define multiple vetted delivery paths in case a delivery path is unavailable or compromised.
- 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 and 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.

#### **4.8.4 Integrators - Technical Implementation Requirements**

- a) Use and check difficult-to-forge marks (such as digital signatures and hologram, DNA, and nano 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 be difficult 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.) at rest and in motion 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 the location 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 and accounting policies.
- e) Consider using multiple sources and compare them, to see if the elements have unexplained differences (e.g., in appearance, performance, or software hash codes).
- f) Document and resolve potential attacks on delivery mechanisms to estimate and evaluate potential loss or compromise of confidentiality, integrity, or availability of elements.

#### **4.8.5 Suppliers - Technical Implementation Requirements**

- a) Use and check difficult-to-forge marks (such as digital signatures and hologram, DNA, and nano 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 be difficult to remove or replace undetected.
- c) Document and monitor the logical delivery of elements, requiring downloading from approved, verification-enhanced sites. Consider encrypting elements (software, software patches, etc.) at rest and in motion throughout delivery. For mechanisms that use cryptographic algorithms, consider compliance with NIST FIPS 140-2.
- d) Document and resolve potential attacks on delivery mechanisms to estimate and evaluate potential loss or compromise of confidentiality, integrity, or availability of elements.

#### **4.8.6 Acquirer - Validation and Verification Activities**

- a) Verify that the integrator has documented processes for the hardening of delivery mechanisms when required, including 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 and element's life cycle.
- b) Review and make recommendations regarding the training of integrator personnel in methods and performance of tasks to harden supply chain delivery mechanisms.
- c) Verify that the delivery processes ensure that only authorized personnel will do the intended transfer and receipt of elements and services.<sup>9</sup>
- d) Verify that the integrator has realistic continuity plans to ensure systems and elements will be available even in a stressed/emergency environment.
- e) Verify that the integrator and supplier have processes that detect significant differences in source materials and ingredients.
- f) Verify that the integrator has processes that detect significant differences in elements.
- g) Perform evaluations of integrator delivery mechanisms for compliance with the processes and procedures implemented to protect the element during production, delivery, and support activities.
- h) Perform periodic evaluations of personnel to ensure compliance with inventory management policies and processes.

#### **4.8.7 Integrators - Validation and Verification Requirements**

- a) Use modeling, simulation, tests, exercises, drills, war games, or Red/Blue 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.

#### **4.8.8 Suppliers - Validation and Verification Requirements**

- a) None

---

<sup>9</sup> ANSI/NASPO-SA-2008

## 4.9 Assure Sustainment Activities and Processes

The sustainment process begins when an element or a system goes operational, and ends when it enters the disposal process. This includes maintenance, upgrade, patching, element replacement (e.g., spare part, alternate supply) and other activities that keep the system or element operational. Any change to the elements, system, or process can introduce opportunities for subversion throughout the supply chain. These changes can occur during any stage of the system or element life cycle. The sustainment processes should limit opportunities and means for compromise of confidentiality, availability, and integrity of elements and operational processes. Acquirer and integrator agreements requirements should include the handling implications of those types of changes as well as protecting, monitoring, and auditing the elements and element processes during operation.

This practice applies to both the bounded operational systems within the acquirers' environment, which may require multitiered supplier operational support, as well as the outsourced operational information system provided by a service provider, which is used remotely by the acquirer. ***Please note that for this practice, the service provider is considered a supplier.*** The integrator is considered a preoperational service provider within the system or element life cycle and is not the focus of this key practice.

A number of security controls contained within NIST SP 800-53, including maintenance and personnel security, provide a baseline of assurances that organizations should employ. The practices described below build on those security controls, particularly those that address FIPS199 high-impact systems.

### 4.9.1 Acquirer – Programmatic Activities

- a) Include procurement clauses in formal service and maintenance agreements with suppliers that reduce supply chain risk.
- b) When acquiring OEM elements, including refurbished elements, establish a contractual relationship with the originator or original manufacturer that provides vetted, competent support where possible.
- c) Where possible (including rapid acquisition), purchase only elements and services previously screened for supply chain risks (including counterfeits/grey market elements and subversion).
- d) 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.
- e) Consider supply chain risks when acquiring replacement elements or field additions/modifications/upgrades, particularly if they do not go through traditional acquisition processes that examine supply chain risks.
- f) For critical elements, perform a more rigorous SCRM review throughout the purchasing process.

- g) Prefer formalized service/maintenance agreement(s) that include:
  - a. Maintenance personnel should meet predefined criteria;
  - b. Use specified or qualified spare parts suppliers;
  - c. Report major changes in a maintenance organization's structure (e.g., physical move to a different location/offshoring, change in ownership, outsourcing, and changes in personnel);
  - d. Provide a complete record of changes performed during maintenance (e.g., audit trail or change log); and
  - e. Review changes made during maintenance.
- h) Establish and implement agreements for competent and suitable support including refurbished and/or salvaged elements, when acquiring elements. Consider requiring the OEM to certify the equipment as suitable.
- i) Identify methods of verifying that service personnel are authenticated and authorized to perform the service work needed at the time.
- j) Require that the system's operational environment will protect the system physically and logically.
- k) Require continuous monitoring activities on the operational system as outlined in NIST SP 800-37 and NIST SP-137.
- l) Include supply chain considerations and requirements in contracts for operational systems and outsourced services.
- m) Require, where applicable, periodic independent third-party audits of elements and systems.
- n) Include applicable system integration and custom code extension activities as part of the upgrade and maintenance efforts in a system's operational requirements and ensure that they are subject to the same rigorous set of testing as originally required.
- o) Develop and implement an approach for handling and processing reported supply chain anomalies.
- p) Require the supplier to identify the expected life span of the element to help the acquirer plan for any migration that might be required in support of continued system and mission operations.
- q) Software is often not warrantied. Some software integrators may be willing to provide service and maintenance agreements such as SLAs, limited warranties, or a maintenance contract. Consider establishing such service agreements for critical software systems. For example, such agreements could include language that the integrator:
  - a. Repair any identified problem if it is a common and widely known security weakness or with significant operational impact. (Examples of such weaknesses may include Open Web Application Security Project [OWASP] top ten [OWASP 2010] or the Common Weakness Enumeration [CWE 2008].)
  - b. Check for preexisting 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.
  - c. If using third-party or open source software, update the software if vulnerabilities in that software are publicly disclosed and patches/updates are available.

- r) Require training on the OEM's procedures for acquiring secondary market (refurbished) items.
- s) Require establishment of a process for managing supply chain vulnerabilities, including detecting, tracking/logging, selecting a response, performing the response, and documenting the response. This provides a feedback loop for continuous improvement of supply chain elements and element processes and corrective action handling for any vulnerability or other issues that require addressing. Similarly, a standardized due process procedure may be needed to ensure that integrators, suppliers, element and sub-suppliers have the opportunity to address and/or appeal any actions that acquirers may seek to impose.
- t) Develop organizational policy and procedures that require that any counterfeit/grey market 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/grey market/subverted elements. If appropriate, share the counterfeit/grey market and subverted elements with the authentic supplier for further analysis.
- u) 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 grey market, potentially counterfeit, and potentially subverted elements.
- v) Avoid use of counterfeit/grey market elements as much as possible.
- w) Establish a formal written policy on software update and patch management. It should articulate the conditions under which updates and patches will be evaluated and administered, such as a change in supplier and the anticipated impact on elements, processes, and uses.
- x) Where relevant, designate and document personnel for physical product purchasing and delivery.
- y) Implement written and repeatable processes for the purchasing, receipt, and delivery of materials for physical element delivery.
- z) Request evidence of the implementation of written, repeatable processes for the purchasing, receipt, and delivery of materials for physical element delivery.
- aa) Use two-person/party review of all orders and shipments, including the comparison of deliverables and receivables to requisition/purchase orders for accuracy of physical product delivery (for example, selection of two individuals from separate departments or duty areas).

#### **4.9.2 Integrators – General Requirements**

None

#### **4.9.3 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 need to be added, implement a vetting process for them. Notify the acquirer of

any major changes in a maintenance organization's structure or process (e.g., physical move to a different location, change in ownership, outsourcing, and/or changes in personnel).

- b) Notify acquirer of any changes in an element's 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.
- c) Establish a process for managing supply chain vulnerabilities including detecting, tracking/logging, selecting a response, performing the response, and documenting the response. This provides a feedback loop for continuous improvement of supply chain elements and element processes.
- d) Implement policies on element software update and patch management. These should articulate the conditions and sources under which updates and patches are delivered or made available to customers.
- e) Document the existence of a process to detect counterfeit/grey market parts in the supply chain. If counterfeit/grey market parts are detected, require that they are seized, destroyed, or preserved for law enforcement evidentiary purposes (not returned to the source/supply chain). Work with the acquirer to ensure counterfeit and subverted elements are subjected to forensic analysis.

#### **4.9.4 Integrators -- Technical Implementation Requirements**

- a) None

#### **4.9.5 Supplier – Technical Implementation Requirements**

- a) Protect system elements from tampering by using a variety of methods. Methods can include robust configuration management, limited privileges, checking cryptographic hashes, and applying anti-tamper techniques.
- b) Establish a trusted baseline for the system/element and operational configuration based on SLAs: Use this baseline to identify unauthorized changes or tampering.
- c) Use existing vulnerability and incident management capabilities to identify potential supply chain vulnerabilities. This provides a feedback loop for continuous improvement of supply chain elements and element processes.
- d) Provide maintenance personnel capable of meeting the terms of the contract.
- e) Ensure that remote maintenance is used only for approved purposes.
- f) Disclose the processes for vulnerability detection including determining root cause and context, determining severity (where feasible), logging, ranking (assigning severity ratings), and triaging security bugs.
- g) Disclose policies on patching and notification, including the criteria for issuances of fix issues (e.g., above a particular CVSS score) prior to product shipment.
- h) Provide trustworthy patch and update processes including the authentication of the patch and or update source (e.g., digitally signed patches).

- i) Perform forensic analysis on failed 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 (include ways to detect prevent future occurrences).

#### **4.9.6 Integrators – Validation and Verification Requirements**

- a) None

#### **4.9.7 Acquirer – Validation and Verification Activities**

- a) Conduct a manual review and inspection, as well as acceptance testing for refurbished or counterfeit/ grey market elements permitted for use. This review and inspection should be conducted during initial procurement and continued throughout operations and sustainment.
- b) Conduct inspection and acceptance testing of incoming items to detect evidence of tampering for physical product delivery.
- c) Review the suppliers' service and maintenance programs and procedures for compliance with contractual requirements.
- d) Evaluate changes in maintenance agreements (e.g., physical move to a different location/offshoring, change in ownership, outsourcing, and changes in personnel) and manage risks associated with them.
- e) Periodically audit supplier system activities for compliance with requirements/SLA and to detect potential supply chain issues. This may include the review of any reports providing a summary of any detection of as malicious functionality, known vulnerabilities, or changes in suppliers or supplier venue - providing a feedback loop for continuous improvement of supply chain elements and element processes.
- f) Monitor and audit the systems and operations to reduce the risk of unauthorized element(s) removal, replacement, and/or modification. Modification review may include applicable system integration and custom code extension activities as part of the upgrade and maintenance efforts for system operations.
- g) Monitor the suppliers of elements of the same family (e.g., similar commoditized elements) to learn of newly discovered vulnerabilities. Provide feedback on relevant, element-specific vulnerabilities to the OEM/supplier for continuous improvement of supply chain elements and element processes.
- h) Verify the digital signatures to ensure that patches are not tampered with during delivery and are applied to the system in the same state as they were when they were produced.
- i) Verify that the delivery mechanism is defined (for example, define the strength of authentication and the encryption mechanism).
- j) Verify the authenticity of patches including nonscheduled or out-of-sequence patches.
- k) Verify that the integrators and suppliers have a protected and access-controlled supply chain risk incident report repository.

#### **4.9.8 Suppliers – Validation and Verification Requirements**

- a) Use multiple and complementary monitoring and auditing approaches and leverage existing data to analyze for supply chain risk during sustainment.
- b) Conduct additional manual review and inspection, as well as acceptance testing, when refurbished or counterfeit/grey market items are permitted for use during initial procurement and continuing through operations and sustainment.
- c) Evaluate the changes in maintenance agreements (e.g., physical move to different location/offshoring, changes in ownership, outsourcing, and change in personnel) and manage risks associated with them.
- d) Identify identical elements coming in from different suppliers as required. For example, if specific orders need to be isolated, the elements from that order can be identified and processed appropriately.
- e) Notify the acquirer and integrator of newly discovered vulnerabilities for continuous improvement of supply chain elements and element processes.
- f) Verify that each patch is either digitally signed or at minimum has a checksum before it is made available to customers.

#### **4.10 Manage Disposal and Final Disposition Activities Throughout the System or Element Life Cycle**

Disposal is a unique practice as it is an activity that can be initiated at any point in the system or element life cycle whether in R&D, requirements definition, development, or operations. Elements, information, and data can be disposed of across the element and system life cycle not only in the disposal or retirement phase of the system or element life cycle. For example, disposal can occur during R&D, design, prototyping, or operations/maintenance and include methods such as disk cleaning, removal of cryptographic keys, partial reuse of components, etc.

This practice addresses both the disposal of elements and tools and documentation in support of elements, processes, and system throughout the system or element life cycle. While poor disposal procedures can lead to unauthorized access to systems and elements, disposal is often performed by actors who may not be aware of supply chain threats or procedures. Opportunities for compromise during disposal affect physical (paper documents) and logical (magnetic) media, as well as the disposal processes themselves. Acquirers frequently neglect to define rules for disposal, increasing chances of compromise caused by lack of planning and control. 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 and provides additional guidance regarding properly addressing supply chain assurance during disposal.

##### **4.10.1 Acquirer - Programmatic Activities**

- a) Ensure disposal requirements are included in contract 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 organizational policies and procedures that :
  - a. Encourage the selection of elements that can be disposed in a way that does not expose protected information. For example, select elements that permit offloading of data prior to disposal or elements that are easy to wipe clean prior to disposal;
  - b. Require the use of trusted disposers, as appropriate (in some cases, they may need to be cleared);
  - c. Require procedures for the secure and permanent destruction of elements, as appropriate; and
  - d. Any counterfeit/grey market parts detected that do not have forensic or evidentiary value should be destroyed by reputable disposers that have been validated by authentic original suppliers or trained law enforcement authorities.
- d) When required for forensic investigations or later comparison for detection of counterfeit/grey market elements, surrender elements for disposal to a dedicated repository.
- e) Establish the end-of-life support process for systems and elements.

#### **4.10.2 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) Prohibit the 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 counterfeit/grey market elements, surrender elements for disposal to a dedicated repository.
- e) Require the 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.

#### **4.10.3 Suppliers - General Requirements**

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

#### **4.10.4 Integrators – Technical Implementation Requirements**

- a) Ensure that scrap materials, out-of-specification elements, or suspect or confirmed defective, counterfeit/grey market, or tampered elements are controlled, preserved for appropriate evidentiary or forensic purposes, and disposed of properly.
- b) Identify all elements and sub-elements that need to be specially disposed of (including Hazardous Materials [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 capabilities for disposal of elements/systems in support of the acquirer's policy, either in an RFI response or in general program support documentation.

#### **4.10.5 Suppliers - Technical Implementation Requirements**

- a) Manage and properly dispose of all scrap materials, out-of-specification elements, or suspected or confirmed defective, counterfeit, or tampered elements.
- b) Establish processes 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).

#### **4.10.6 Acquirer - Validation and Verification Activities**

- a) Assess the integrators' and suppliers' capability to meet the disposal requirements.
- b) Periodically review the acquirer's organizational disposal process.
- c) Ensure the adequacy of the destruction method for controlled items.

#### **4.10.7 Integrators - Validation and Verification Requirements**

- a) Ensure the adequacy of the destruction method for controlled items.
- b) Verify suppliers' 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.

#### **4.10.8 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.

DRAFT

## APPENDIX A GLOSSARY

<b>Term</b>	<b>Definition</b>	<b>Source</b>
Access	Ability to make use of any information system resource.	NISTIR 7298
Acquirer	Stakeholder that acquires or procures a product or service.	ISO/IEC 15288, adapted
Acquisition	Includes all stages of the process of acquiring product or services, beginning with the process for determining the need for the product or services and ending with contract completion and closeout.	NIST SP 800-64, adapted
Authorizing Official (AO)	Senior federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.	CNSSI-4009
Baseline	Hardware, software, databases, and relevant documentation for an information system at a given point in time.	CNSSI-4009
Commercial off-the-shelf (COTS)	Software and hardware that already exists and is available from commercial sources. It is also referred to as off-the-shelf.	NIST SP 800-64
Contract	A mutually binding legal relationship obligating the seller to furnish the supplies or services (including construction) and the buyer to pay for them. It includes all types of commitments that obligate the Government to an expenditure of appropriated funds and that, except as otherwise authorized, are in writing. In addition to bilateral instruments, contracts include (but are not limited to) awards and notices of awards; job orders or task letters issued under basic ordering agreements; letter contracts; orders, such as purchase orders, under which the contract becomes effective by written acceptance or performance; and bilateral contract modifications. Contracts do not include grants and cooperative agreements covered by 31 U.S.C. 6301, et seq.	48 CFR
Contract administration office	An office that performs— (1) Assigned post-award functions related to the administration of contracts; and (2) Assigned pre-award functions.	48 CFR
Contracting office	An office that awards or executes a contract for supplies or services and performs post-award functions not assigned to a contract administration office (except as defined in 48 CFR).	48 CFR
Contracting Officer (CO)	An individual who has the authority to enter into, administer, or terminate contracts and make related determinations and findings.	Federal Acquisition Regulation
Critical Component	A system element that, if compromised, damaged, or failed, could cause a mission or business failure.	
Defense-in-Breadth –	A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and	CNSSI-4009

	retirement).	
Defense-in-Depth –	Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.	CNSSI-4009; NIST SP 800-53
Defensive design	Design techniques which explicitly protect supply chain elements from future attacks or adverse events. Defensive design addresses the technical, behavioral, and organizational activities. It is intended to create options that preserve the integrity of the mission and system function and its performance to the end user or consumer of the supply chain element.	
Degradation	A decline in quality or performance; the process by which the decline is brought about.	
Down Select	To narrow the field of choices; a reduction in the number of contractors or sub-contractors, as a project moves from one phase to another, in accordance with established criteria.	
Element	Commercial off-the-shelf (COTS) or government off-the-shelf (GOTS) software, hardware or firmware. Synonymous with components, devices, products, systems, and materials.	
Element Processes	A series of operations performed in the making or treatment of an element; performing operations on elements/data.	
Federal Acquisition Regulation (FAR)	The Federal Acquisition Regulations System is established for the codification and publication of uniform policies and procedures for acquisition by all executive agencies.	48 CFR
Federal Information Processing Standards	A standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability.	NIST SP 800-64
Grey (or grey) market	An unofficial, unauthorized, or unintended distribution channel.	
High Impact	The loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; (i.e., 1) causes a severe degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; 2) results in major damage to organizational assets; 3) results in major financial loss; or 4) results in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries).	FIPS 199; CNSSI-4009

ICT Supply Chain	Linked set of resources and processes between acquirers, integrators, and suppliers that begins with the sourcing of ICT products and services and extends through the manufacturing, processing, design, development, handling, and delivery of ICT products and services to the acquirer.	ISO 28001 , adapted
ICT Supply Chain Risk	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.	NIST SP 800-53 Rev 3: FIPS 200, adapted
Identity	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.	CNSSI No. 4009
Industrial Security	The portion of internal security that refers to the protection of industrial installations, resources, utilities, materials, and classified information essential to protect from loss or damage.	NISPOM, adapted
Information and Communications Technologies (ICT)	Encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information.	ANSDIT, adapted
Information Assurance (IA)	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.	CNSSI No. 4009
Integrator	An organization that customizes (e.g., combines, adds, optimizes) elements, processes, and systems. The integrator function can be performed by acquirer, integrator, or supplier organizations.	
Life cycle	Evolution of a system, product, service, project, or other human made entity from conception through retirement.	ISO/IEC 15288
Low Impact	The loss of confidentiality, integrity, or availability that could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; (i.e., 1) causes a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; 2) results in minor damage to organizational assets; 3) results in minor financial loss; or 4) results in minor harm to individuals).	CNSSI-4009
Market research	Collecting and analyzing information about capabilities within the market to satisfy agency needs.	48 CFR

Moderate Impact	The loss of confidentiality, integrity, or availability that could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; (i.e., 1) causes a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; 2) results in significant damage to organizational assets; 3) results in significant financial loss; or 4) results in significant harm to individuals that does not involve loss of life or serious life threatening injuries).	CNSSI-4009
Modular Contracting	Under modular contracting, an executive agency’s need for a system is satisfied in successive acquisitions of interoperable increments. Each increment complies with common or commercially accepted standards applicable to information technology so that the increments are compatible with other increments of information technology comprising the system.	U.S. Code Title 41
Procurement	(see “acquisition”).	48 CFR
Provenance	The records describing the possession of, and changes to, components, component processes, information, systems, organization, and organizational processes. Provenance enables all changes to the baselines of components, component processes, information, systems, organizations, and organizational processes, to be reported to specific actors, functions, locales, or activities.	
Red Team/Blue Team Approach	<p>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.</p> <p>1. The group responsible for defending an enterprise’s use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team). Typically the Blue Team and its supporters must defend against real or simulated attacks 1) over a significant period of time, 2) in a representative operational context (e.g., as part of an operational exercise), and 3) according to rules established and monitored with the help of a neutral group refereeing the simulation or exercise (i.e., the White Team).</p> <p>2. The term Blue Team is also used for defining a group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on the Blue Team findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the customer's cyber security readiness posture. Often times a Blue</p>	CNSSI 4009

	Team is employed by itself or prior to a Red Team employment to ensure that the customer's networks are as secure as possible before having the Red Team test the systems.	
Risk Management	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.	NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.	CNSSI-4009
Sources Sought Notice (SSN)	A synopsis posted by a government agency that states they are seeking possible sources for a project. It is not a solicitation for work, nor is it a request for proposal.	FAR, Subpart 7.3 and OMB Circular A-76
Statement of Work (SOW)	The SOW details what the developer must do in the performance of the contract. Documentation developed under the contract, for example, is specified in the SOW. Security assurance requirements, which detail many aspects of the processes the developer follows and what evidence must be provided to assure the organization that the processes have been conducted correctly and completely, may also be specified in the SOW.	NIST SP 800-64
Supplier	Organization or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain.	ISO/IEC 15288, adapted
System	A combination of interacting elements organized to achieve one or more stated purposes.	ISO/IEC 15288:2008
System Assurance	The justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle.	NDIA 2008
System Development Life Cycle (SDLC)	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.	NIST SP 800-34; CNSSI-4009
System Owner	Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.	CNSSI-4009
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	NIST SP 800-53; NIST SP 800-53A; NIST SP 800-27; NIST SP 800-60; NIST SP 800-37; CNSSI-4009
Threat Assessment/Anal	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the	CNSSI-4009; SP 800-53A

ysis	threat.	
Threat Source	A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time	Draft NIST 800-30 Rev. 1
Threat Scenario	A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time.	Draft NIST 800-30 Rev.1
Trust	The confidence one element has in another, that the second element will behave as expected.	Software Assurance in Acquisition: Mitigating Risks to the Enterprise, NDU, October 22, 2008.
Validation	Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled.	ISO 9000
Verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome).	CNSSI-4009, ISO 9000, adapted
Visibility (also Transparency)	A property of openness and accountability throughout the supply chain.	ISO/IEC 27036-3 Draft, adapted
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.	NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-60; NIST SP 800-115; FIPS 200
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.	NIST SP 800-53A; CNSSI-4009

**APPENDIX B ACRONYMS**

AO –	Authorizing Official
CCR –	Central Contractor Registry
CIO –	Chief Information Officer
CISO –	Chief Information Security Officer
CM –	Configuration Management
CNCI –	Comprehensive National Cybersecurity Initiative
CNSS –	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CO –	Contracting Officer
COTS –	Commercial Off-The-Shelf
COTR –	Contracting Officer’s Technical Representative
CRADA –	Cooperative Research and Development Agreement
CWE –	Common Weakness Enumeration
DHS –	Department of Homeland Security
DISA –	Defense Information Systems Agency
DoD –	Department of Defense
DUNS –	Dun and Bradstreet
FAR –	Federal Acquisition Regulation
FDCC –	Federal Desktop Core Configuration
FIPS –	Federal Information Processing Standards
GITWG –	Global Information Technology Working Group
GOTS –	Government Off-The-Shelf
GSA –	General Services Administration
HAZMAT –	Hazardous Materials
IA –	Information Assurance

ICT –	Information and Communication Technology
IEC –	International Electrotechnical Commission
IP –	Internet Protocol
ISO –	International Organization of Standardization
IT –	Information Technology
ITL –	Information Technology Laboratory (NIST)
MTBF –	Mean-time-between-failures
NASPO –	North American Security Products Organization
NDIA –	National Defense Industrial Association
NIST –	National Institute of Standards and Technology
NSA –	National Security Agency
OEM –	Original Equipment Manufacturer
OMB –	Office of Management and Budget
OWASP –	Open Web Application Security Project
R&D –	Research and Development
RFI –	Request for Information
RFP –	Request for Proposal
RFQ –	Request for Quote
SAISO –	Senior Agency Information Security Officer
SCAP –	Security Content Automation Protocol
SCRM –	Supply Chain Risk Management
SDLC –	System Development Life cycle
SLA –	Service-Level Agreement
SOO –	Statement of Objectives
SOP –	Standard Operating Procedure
SOW –	Statement of Work
SSN –	Sources Sought Notice

STIG –	Security Technical Implementation Guides
T&E –	Test and Evaluation
U.S. –	United States (of America)
USGCB -	United States Government Configuration Baseline

DRAFT

## APPENDIX C REFERENCES

The Common Criteria Evaluation and Validation Scheme, *Home Page 2008*, URL: <http://www.niap-ccevs.org/cc-scheme/>, accessed December 5, 2011.

Software Assurance Community Resources and Information Clearinghouse Sponsored by the Department of Homeland Security Cyber Security Division, URL: <http://buildsecurityin.us-cert.gov>, accessed December 5, 2011.

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/Pages/Search.aspx?k=12012008.pdf>, accessed November 7, 2011.

Committee on National Security Systems (CNSS) Instruction 4009, *National Information Assurance (IA) Glossary*, Revised April 2010, URL: [http://www.cnss.gov/Assets/pdf/cnssi\\_4009.pdf](http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf), accessed November 7, 2011.

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/index.html>, accessed December 5, 2011.

DHS National Cyber Security Division *Security in the Software Lifecycle: Making Software Processes and the Software Produced by Them – More Secure, Section 3.5 and Appendix G: G.5*. Draft Version 2.1, August 2006.

Acquisition Central, Sponsored by U.S. General Services Administration, Federal Acquisition Regulation, URL: <https://www.acquisition.gov/far/>, Accessed November 7, 2011.

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](http://www.iso.org/iso/catalogue_detail?csnumber=43562), accessed December 5, 2011.

International Organization for Standardization, *Specification for Security management systems for the supply chain*, 2007, URL:

[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=44641](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44641).

International Organization for Standardization, *Quality management systems: Requirements*, 2008, URL:

[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=46486](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46486).

Management Pilot Program. February 25, 2010. National Defense Industrial Association (NDIA), *Engineering for System Assurance*, September 2008, version 1.0, aka *NDIA System Assurance Guidebook*, <http://www.acq.osd.mil/se/docs/SA-Guidebook-v1-Oct2008.pdf>, accessed December 5, 2011.

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](https://buildsecurityin.us-cert.gov/swa/downloads/SwA_in_Acquisition_102208.pdf), accessed December 5, 2011.

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, Draft Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, September 19, 2011.

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, Draft Special Publication 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems*, December 2011.

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 2, *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*, February 2011.

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, Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011.

Open Web Application Security Project (OWASP) Top 10 Project, 2007, URL: [http://www.owasp.org/index.php/Top\\_10\\_2007](http://www.owasp.org/index.php/Top_10_2007); accessed December 5, 2011.

OSSTMM – Open Source Security Testing Methodology Manual, <http://www.isecom.org/osstmm/>; accessed December 5, 2011.

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

SafeCode, *Fundamental Practices for Secure Software Development*, October 8, 2008, URL, [http://www.safecode.org/publications/SAFECode\\_Dev\\_Practices1108.pdf](http://www.safecode.org/publications/SAFECode_Dev_Practices1108.pdf), accessed December 5, 2011.

Business for Social Responsibility: *Perspectives on Information Management in Sustainable Supply Chains*. [http://www.bsr.org/reports/BSR\\_Info-Management-Supply-Chains1.pdf](http://www.bsr.org/reports/BSR_Info-Management-Supply-Chains1.pdf); accessed September 2, 2011.

O'Connor, Christopher J. *Transparency – what does it mean to the supply chain?* from [www.nexeraconsulting.com/60/File.aspx](http://www.nexeraconsulting.com/60/File.aspx); accessed September 2, 2011.

DRAFT

## APPENDIX D UMD ICT SUPPLY CHAIN STUDY



# ASSESSING SCRM CAPABILITIES AND PERSPECTIVES OF THE IT VENDOR COMMUNITY: TOWARD A CYBER-SUPPLY CHAIN CODE OF PRACTICE

EXECUTIVE SUMMARY



UNIVERSITY OF  
MARYLAND

ROBERT H. SMITH  
SCHOOL OF BUSINESS

# Executive Summary

## *I. Project Concept*

Initiative 11 (Supply Chain Risk Management) of the President's Comprehensive National Cybersecurity Initiative (CNCI) tasked the National Institute of Standards and Technology (NIST) with integrating lessons learned about cyber supply chain practices from various federal and industry initiatives into guidance for the federal enterprise and its industry partners.

NIST's Information Technology Lab awarded the Supply Chain Management Center of the Robert H. Smith School of Business at the University of Maryland in College Park a grant in support of the development of cyber supply chain best practice guidelines by NIST. In October, 2010, the Supply Chain Management Center began work on a project to develop, validate, and pilot test a research tool to assess the cyber-supply chain capabilities of the IT vendor community.

This grant was aimed at addressing the fact that, at present, no readily identifiable assessment tool for industry exists that, if used extensively, could form the basis for a body of cyber-supply chain knowledge. Such a body of knowledge should contain data about current/planned corporate risk governance mechanisms, risk management audit/compliance activities, and benchmark practices against which to audit the capability and maturity of an organization.

This lack of a data-driven body of knowledge has been a major deficiency in the emerging discipline of Cyber-Supply Chain Risk Management (SCRM) and has constrained sound decision-making across government and the private sector. It was hoped that data gathered from this project could contribute to the formulation of a straw man SCRM Code of Practice that could advance the discipline and serve as a basis for ongoing dialogue between the public and private sectors.

## *II. Project Methodology*

This project developed a tool to assess cyber-supply chain risk management capabilities by consolidating the collective inputs of the set of public and private actors engaged in supporting Initiative 11. The Department of Commerce (NIST and Bureau of Industry and Security, BIS), the Department of Homeland Security (DHS); the Department of Defense (DOD/CIO and DOD/NSA); and the Government Services Administration all provided formal inputs to design the assessment tool. Representatives from Safe Code and Tech America's SCRM sub-committee also contributed valuable inputs.

This tool was then distributed to and validated with a sample of vendors of IT systems, software, hardware, and services. Our target participants included: small to medium-sized IT vendors traditionally under-represented in IT surveys; Chief Information Officers/Chief Security Officers nationally and in the Washington DC region; and Directors of Supply Chain.

There were 131 respondents who completed the survey from beginning to end. This means our survey response rate equaled the 1% industry benchmark for Third Party IT Surveys (source: IDG List Services). This is especially impressive given the absence of official survey distribution; the length of time it takes to fill in the survey (approximately 30 minutes); the newness of the subject discipline; and the difficulties some companies reported in routing the survey to appropriate person(s) in the organization. An additional 159 respondents completed one or more sections of the survey. In total, 290 surveys were either partially or fully completed.

### **III. Key Results**

#### ***Respondent Characteristics***

Sample of research respondents reflects the fact that a number of different functional areas within firms are addressing the cyber-supply chain problem. As expected, professionals in IT, Telecom Services, and Information Security represent 63.4% of the sample, while professionals in Supply Chain Management, Procurement/Acquisition, and Risk Management accounted for an additional 36.6% of the sample.

Our respondent sample is dominated by small companies with less than \$20 million in revenues, who represent 71% of the sample. By contrast, large companies with annual sales greater than \$1 billion represent 10.3% of the sample. We believe these results represent one of the first times survey research in the cyber-community has reached beyond Tier 1 product companies and prime vendor/ integrators.

Software was cited as a line of business by 48.6% of respondents; hardware by 31.4%; telecom/data networking by 24.8%; and system integration services by 62.4% of the sample.

We found that 55.4% of companies with annual sales of less than \$20 million reported working across four or more IT product/service areas. We interpret this to mean that even very small companies are increasingly focused on the development and deployment of systems across traditional product/service boundaries. It also implies a trend to increasing IT Sector-wide managerial complexity. This complexity invariably leads to higher risk profiles across all classes of firms as broader sets of supply chain assets/resources need to be continuously protected from cyber threats.

About 86.8% of respondents currently serve and plan to serve the federal government.

#### ***Respondent SCRM Practices***

Research results demonstrated that there is significant difference between the extent of use of strategic risk management practices in the IT supply chain and more tactical, or field level practices.

On the strategic side of risk management, 47.6% of the sample *never* uses a Risk Board or other executive mechanisms to govern enterprise risk; 46.1% *never* uses a shared risk registry/ an online database of IT supply chain risks; and 49.4% *never* uses an integrated IT supply chain dashboard/control. Even if we take away the requirement of real time supply chain systems, 44.9% say they *never* use a supply chain risk management plan.

The adaption of strategic risk management actions that does occur seems to be the province of big companies: the greater the company revenue, the greater the propensities to always or often use strategic risk measures. Only 17% of the smallest companies said they always or often use real time dashboards; compared to 50% of the biggest companies. Only 7% of smallest companies used on line risk registries always or often, compared to 63.2% of the biggest companies.

There appears to be a huge gulf between the smallest companies and the biggest companies who appear to have more real time information access and who tend to deploy that information as part of sense and respond cyber supply chain operations. One contributory factor might be that bigger companies are more risk and liability-sensitive. Additionally, they can invest more in sophisticated threat analysis techniques and in implementing enterprise-wide risk governance programs. On the other hand, more tactical, narrowly focused cyber-SCRM practices are used much more often or always. Indeed, 67.3% of the sample often or always do personnel security reviews; 57.3% often or always use perimeter detection systems; and 49.4% often or always use a standardized process for pre-qualifying suppliers.

These more tactical defense mechanisms are indicative of single enterprise protection mechanisms, which may, in concert with other activities, provide some measure of defense in depth. However, they are not implemented with defense in breadth in mind; and can be perceived to lack the necessary executive management buy-in to influence customers and suppliers.

This deficiency of extended enterprise SCRM was further highlighted by the lack of collaboration among key actors within a supply chain evidenced in our sample: Companies report little or no collaboration with key suppliers: for example, 51.5% of companies in the sample provide no access to planning systems for their suppliers. Even the most widely accepted SCRM practice “jointly monitoring current changes, incidents, exceptions and disruptions” was only extensively used by 28.8% of the sample, less than a third of the respondents

The results seem clear: there is an overall lack of corporate emphasis on strategic defense in breadth and extended enterprise management of supply chain risks. Companies of all sizes tend to focus heavily on field-level technical practices.

### ***Attractiveness Of Code Of Practice Elements***

Finally, we asked respondents to rate the attractiveness of items for potential inclusion into a Code of Practice for IT Vendors that seeks to improve supply chain risk management. Attractiveness was defined as an index score blending both operational effectiveness and feasibility of implementation.

We found a straightforward correlation: the greater the corporate revenue, the greater the corporate support for Code of Practice elements that are strategic in scope, e.g. Risk Boards and Risk Plans. Also, the largest companies are especially interested in obtaining government-designated favored supplier status: 91.7% of them rated priority

status as the most effective/highly effective potential Code element as compared to 57.2% of the smallest companies.

There was across the board support for inclusion of elements that “provide additional contractual resources for SCRM” and “streamline regulations” into a Code of Practice.

On one hand, there is this desire on the part of companies of all sizes for streamlined, less burdensome or obtuse regulations and less government intervention. Yet, on the other hand, we found widespread support for government actions and information to clarify:

- What is the real threat?
- What are priority SCRM practices?
- How can expanded use of those practices by companies tie into to real corporate benefits, such as reduction of liability and overall compliance costs?

Successfully answering the latter question is especially crucial for successful adoption of a Cyber-Supply Chain Code of Practice

#### ***IV. Conclusions***

There are a few critical conclusions that can be drawn from our research:

##### Both Large & Small Companies Seriously Under-Manage Cyber-SCRM

Both small and big companies increasingly work across hardware and software development, network management, and systems integration boundaries and have multiple product/service offerings. In other words, companies of all sizes have become complex supply chains with highly dispersed assets and resources.

Given the challenge of escalating cyber supply chain complexity, the current state of corporate SCRM capability seems inadequate for managing *systemic risk*. The deficiency of cyber supply chain-wide risk governance strategies; the stove piped nature of risk management, cyber security and supply chain functions within corporations of all sizes; and an ongoing industry orientation toward narrowly focused process-models and technical solutions- all present serious impediments to effective SCRM in the current era.

##### Both Large & Small Companies Can Be Incentivized To Improve Cyber-SCRM

Small companies are highly motivated to get and use government cyber-supply chain risk management practice guidelines. This helps them to win business with the federal acquirer community; as well as to conserve scarce dollars and management time that they would otherwise have to spend themselves on cyber security compliance research.

Although their cyber security units are not well integrated into or supported by corporate risk management programs, big companies are nevertheless highly sensitive to managing regulatory demands for risk assurance and seeking to limit their own corporate liability. This sensitivity to risk and the search for shielding mechanisms have certainly been major motivating factors in developing Codes of Practice in other non-IT industries, such as the chemical industry (Code of Responsible Care) and the consumer products industry (Supply Chain Operations Reference Model).

Key challenges going forward include identifying and deploying the best incentive strategies available to assure maximum diffusion of and compliance with a core set of cyber-SCRM best practices. Such strategies might include: defining liability limits in cyber-supply chains; encouraging industry risk pooling to free up company-level capital reserves currently held for future liability claims or uninsurable risks; and implementing legislative/regulatory streamlining initiatives that ease industry compliance costs while building assurance levels.

Only by going forward together, can government and industry master the extreme challenges of cyber-SCRM in a global era.

DRAFT